ALEOS 4.3.4 Software Configuration

User Guide

4114514
Rev 1

Important Notice

Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors) or be totally lost. Although significant delays or losses of data are rare when wireless devices such as the Sierra Wireless modem are used in a normal manner with a well-constructed network, the Sierra Wireless modem should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. Sierra Wireless accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the Sierra Wireless modem, or for failure of the Sierra Wireless modem to transmit or receive such data.

Safety and Hazards

Do not operate the Sierra Wireless modem in areas where blasting is in progress, where explosive atmospheres may be present, near medical equipment, near life support equipment, or any equipment which may be susceptible to any form of radio interference. In such areas, the Sierra Wireless modem **MUST BE POWERED OFF**. The Sierra Wireless modem can transmit signals that could interfere with this equipment.

Note: Some airlines may permit the use of cellular phones while the aircraft is on the ground and the door is open. Sierra Wireless modems may be used at this time.

The driver or operator of any vehicle should not operate the Sierra Wireless modem while in control of a vehicle. Doing so will detract from the driver or operator's control and operation of that vehicle. In some states and provinces, operating such communications devices while in control of a vehicle is an offence.

Limitation of Liability

The information in this manual is subject to change without notice and does not represent a commitment on the part of Sierra Wireless. SIERRA WIRELESS AND ITS AFFILIATES SPECIFICALLY DISCLAIM LIABILITY FOR ANY AND ALL DIRECT, INDIRECT, SPECIAL, GENERAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR REVENUE OR ANTICIPATED PROFITS OR REVENUE ARISING OUT OF THE USE OR INABILITY TO USE ANY SIERRA WIRELESS PRODUCT, EVEN IF SIERRA WIRELESS AND/OR ITS AFFILIATES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR THEY ARE FORESEEABLE OR FOR CLAIMS BY ANY THIRD PARTY.

Notwithstanding the foregoing, in no event shall Sierra Wireless and/or its affiliates aggregate liability arising under or in connection with the Sierra Wireless product, regardless of the number of events, occurrences, or claims giving rise to liability, be in excess of the price paid by the purchaser for the Sierra Wireless product.

Patents

This product may contain technology developed by or for Sierra Wireless Inc. This product includes technology licensed from QUALCOMM®. This product is manufactured or sold by Sierra Wireless Inc. or its affiliates under one or more patents licensed from InterDigital Group and MMP Portfolio Licensing.

Copyright

© 2013 Sierra Wireless. All rights reserved.

Trademarks

Sierra Wireless®, AirPrime®, AirLink®, AirVantage® and the Sierra Wireless logo are registered trademarks of Sierra Wireless.

Watcher® is a registered trademark of NETGEAR®, Inc., used under license.

Windows® and Windows Vista® are registered trademarks of Microsoft Corporation.

Macintosh® and Mac OS X® are registered trademarks of Apple Inc., registered in the U.S. and other countries.

QUALCOMM® is a registered trademark of QUALCOMM Incorporated. Used under license.

Other trademarks are the property of their respective owners.

Contact Information

International Contact Information

Please contact your AirLink Reseller for technical support.

AirLink Sales	airlinksales@sierrawireless.com
AirLink Support	support@sierrawireless.com
AirLink RMA Repairs	repairs@sierrawireless.com
AirLink Online Support Knowledgebase	www.sierrawireless.com/Support/SupportCenter
AirLink Software Downloads	www.sierrawireless.com/Support/Downloads
Corporate Web Site	www.sierrawireless.com

Sierra Wireless Headquarters Contact Information

Postal Address:	Sierra Wireless 13811 Wireless Way Richmond, BC Canada V6V 3A4

Consult our website for up-to-date product descriptions, documentation, application notes, firmware upgrades, troubleshooting tips, and press releases:

www.sierrawireless.com

Contents

Introduction 13

Overview 13

Sierra Wireless AirLink Products 13

About Documentation 14

Tools and Reference Documents 15

Device Configuration 17

Main Menu Tabs 18

Configuring 18

Creating a Template 19

Applying a Template 20

AT Command Mode 22

SSH PAD Mode 22

Server Configuration 23

Update the ALEOS Software and Radio Module Firmware 28

Step 1—Planning Your Update 28

Recommendations 31

Step 2—Update the ALEOS Software and Radio Module Firmware 31

Enterprise LAN Management 37

Configuring Your Device for use in a PCI Compliant System 38

Status 41

Home 41

WAN/Cellular 47

LAN 55

LAN/WiFi 56

VPN 58

Security 59

Services 59

GPS 60
Serial 62
Applications 64
About 64

LAN/Wi-Fi Configuration 67
Private and Public Mode 67
DHCP/Addressing 70
Ethernet 74
USB 76
Installing the USB Drivers for Windows 78
Host Port Routing 84
Wi-Fi 85
Access Point Mode 86
Client Mode 90
Both (AP + Client) Mode 92
Global DNS 93
PPPOE 94
Configure the AirLink Device to Support PPPoE 95
Configuring a PPPoE Connection in Windows 7 96
VLAN 99
VRRP 100
Host Interface Watchdog 101

WAN/Cellular Configuration 103
Re-Activation 118
Backup APN 119
Reliable Static Routing (RSR) 119

VPN Configuration 123
IPsec 123
Split Tunnel 124

VPN 1 124
IPsec 125
GRE 128
SSL Tunnel 129
VPN 2 to VPN 5 132

Security Configuration 133
Solicited vs. Unsolicited 133
Port Forwarding 133
DMZ 137
Port Filtering—Inbound 139
Port Filtering — Outbound 140
Trusted IPs—Inbound (Friends) 140
Trusted IPs—Outbound 142
MAC Filtering 142
Packet Inspection 143

Services Configuration 145
AVMS (AirVantage Management Service) 145
ACEmanager 146
Low Power 147
Dynamic DNS 151
Understanding Domain Names 155
Dynamic Names 156
WiFi Landing Page 157
SMS 157
Password Only 158
Control Only 159
Gateway Only 161
Control and Gateway 164

SMS Wakeup 168
SMS Security 169
Inbound SMS Messages 169
Trusted Phone Number 171
SMS Password Security 171
SMS > Advanced 173
SMSM2M 174
Telnet/SSH 175
Email (SMTP) 176
Management (SNMP) 177
Time (SNTP) 182
Device Status Screen 183

GPS Configuration 185
GPS Overview 185
ALEOS Supported GPS Report Protocols 186
Before Configuring GPS 186
Servers 1 to 4 187
Local/Streaming 198
Local/Streaming—LATS 200
Global Settings 204

Events Reporting Configuration 207
Introduction 207
Additional Behavior and Features 208
Configuration Overview 208

Action Description 213
Action Type 213
Email/SMS 216
Report Groups 216
Relay 219
Configure Events 219
Events Protocol 220

Serial Configuration 221
Port Configuration 221
Port Configuration 222
Reverse Telnet/SSH 224
UDP Multiple Unicast 227
Advanced 228
TCP 230
UDP 232
PPP 234
Modbus Address List 234
I/O X-Card Serial Port Configuration 235
Advanced Settings 238
TCP Settings 239
UDP Settings 241

Application Configuration 243
Data Usage 243
Garmin 248
ALEOS Application Framework 250

I/O Configuration 253
Current State 255
Pulse Count 256

Configuration 257
Transformed Analog 258

Admin 261
Change Password 261
Advanced 261
Radio Passthru 263
Log 264

Windows Dial-up Networking (DUN) 267
Installing a Device Driver 267
Creating a Dial-Up Networking (PPP) Connection 277
Connecting to the Internet Using DUN 286
ACEview 286
Windows DUN 287

Modbus/BSAP Configuration 289
Modbus Overview 289
Configuring the AirLink Device at the Polling Host for Modbus on UDP 291
Configuring the Remote AirLink Devices for Modbus with UDP 292

SNMP: Simple Network Management Protocol 295
Management Information Base (MIB) 295
SNMP Traps 295
Sierra Wireless MIB 295

AT Commands 321
AT Command Set Summary 321
Reference Tables 322
Device Updates 323

Status 323
WAN/Cellular 328
LAN/WiFi 334
LAN 334
Wi-Fi 336
VPN 339
Security 344
Services 345
GPS 353
Serial 359
Standard (Hayes) commands 366
I/O. 371
Applications 372
Admin 373

SMS Commands 377
SMS Command format. 377
List of SMS Commands 378

Q & A and Troubleshooting 381
ACEmanager Web UI 381
Ethernet Ports 381
LAN Networks 381
Wi-Fi 382
Port Forwarding 382
ALEOS Application Framework (ALEOS AF) 383
SMS 383
GPS 383
Error Reporting 384
VPN 384
Poor Wireless Network Connection 385
Connection not working 386
Updating the ALEOS Software and Radio Module Firmware 386
TCP Connections 394
AirVantage Management Service 395
LTE Networks 396
SIM Card is Blocked 397
Remote connections 398
Radio Band Selection 398
Reliable Static Routing (RSR) 399

Glossary of Terms 401

Index. 407

1: Introduction

1

Note: This user guide is intended for the AirLink LS300 and the AirLink GX Series devices. If you have an AirLink ES440, refer to the ALEOS Software Configuration User Guide for the AirLInk ES440.

Overview

ACEmanager™ is the free, web-based utility used to manage and configure the AirLink® device. It is a web application integrated in the ALEOS™ software that runs on the AirLink device. AirLink Embedded Operating System (ALEOS) is purpose-built to maintain a wireless connection and to configure the gateway to the needs of the system. ACEmanager provides comprehensive configuration, monitoring, and control functionality to all AirLink gateways and routers.

ACEmanager enables you to:

- Login and configure device parameters
- Adjust network settings
- Change security settings
- Update events reporting and control outputs
- Update ALEOS software and radio module firmware
- Copy configuration settings to other AirLink devices

Since ACEmanager can be accessed remotely over-the-air as well as locally, the many features of ALEOS can be managed from any location.

An ALEOS configuration template can be created using ACEmanager, after a single device is configured and installed, to program other AirLink gateways with the same configuration values. This enables quick, accurate deployment of large pools of devices.

Sierra Wireless AirLink Products

ACEmanager is intended to be used with the following products with ALEOS:

- AirLink GX Series
- AirLink LS300
- AirLink ES440

Choosing the right product for your needs

	AirLink ES440	AirLink GX Series	AirLink LS300
Target Application	Enterprise (office, remote store, point-of-sale, etc.)	Mobile and Industrial (police, fire, fleets and oil, gas, rail, remote access)	Industrial (oil and gas utilities, remote solar panels)
Location	No GPS	GPS	GPS
Ingress Protection	n/a	IP64	n/a
Hazardous Location	n/a	Class 1 Div.2	Class Div. 2
Operating Temperature	0° to 40°C	-30° to +70°C	-30° to +70°C
Shock and Vibration	1 m drop test, non-operational	Military Standard 810	Military Standard 810
Serial Features	Serial port: Reverse Telnet for OOBM	Serial Byte protocol support (DNP3, Modbus, BSAP, DF1 [Allen-Bradley])	Serial Byte protocol support DNP3, Modbus, BSAP, DF1 [Allen-Bradley])
Power	AC power only (12VDC)	AC and DC power (9–36VDC)	AC and DC power
Input/Output	No optional I/O	Optional I/O	Limited I/O
Events Reporting	SNMP Trap events only	Full Events Reporting, SMS Events Reporting	Full Events Reporting, SMS Events Reporting
Warranty	1 Year Warranty (Optional 3 Year Warranty)	5 Year Warranty	3 Year Warranty

For more information on specific AirLink products, refer to the hardware user guide, available from www.sierrawireless.com/en/Support/Downloads.aspx.

About Documentation

Each chapter in the ALEOS Configuration User Guide describes a section (a tab in the user interface) of ACEmanager.

Chapters in this user guide explain:

- Parameter descriptions in ACEmanager
- Relevant configuration details
- User scenarios for certain sections in the guide.

This User Guide is kept up to date and provided as a PDF (Portable Document Format) file on the Sierra Wireless support website.

Tools and Reference Documents

Document	Description
AirLink Device User Guide	This hardware document describes how to: • Install the AirLink device hardware • Connect the radio antennas • Connect a notebook computer and other input/output (I/O) devices • Interpret the LEDs and indicators on the AirLink device.
ACEview User Guide	This document explains how to use the ACEview utility to monitor the connection state of a Sierra Wireless AirLink device and GPS or power status as applicable.
AVMS User Guide	This document explains how to use AirVantage Management Service for the remote management of Sierra Wireless AirLink devices.

2: Device Configuration

To access ACEmanager:

1. Insert the SIM card, if applicable. Refer to the AirLink device user guide for details.
2. Power on the AirLink device.
3. Launch your browser and enter the IP address and port number http://192.168.13.31:9191
4. Log in:
   - User Name: “user” (entered by default) or “viewer

     Use the “user” login for configuring or monitoring your device.

     Logging in as “viewer” only allows you to view the configuration and connection state. You cannot make any configuration changes.
   - Default Password: 12345

Note: ACEmanager has a 15 minute timeout. After 15 minutes of inactivity, you are redirected to the login screen.

To prevent others from changing the AirLink device settings, you can change the ACEmanager password (Chapter 14).

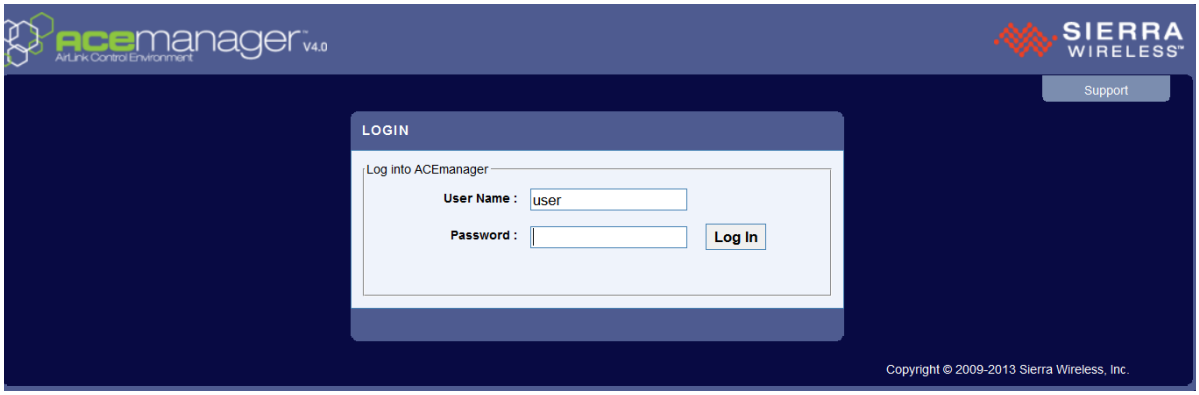


Figure 2-1: ACEmanager: Main Login screen

After your initial login to ACEmanager, you have the option of displaying the device status parameters on subsequent login screens.

5. In ACEmanager, go to Services > Device Status Screen.
6. In the Device Status on Login Screen field, select Enable. (For details, see Device Status Screen on page 183.)

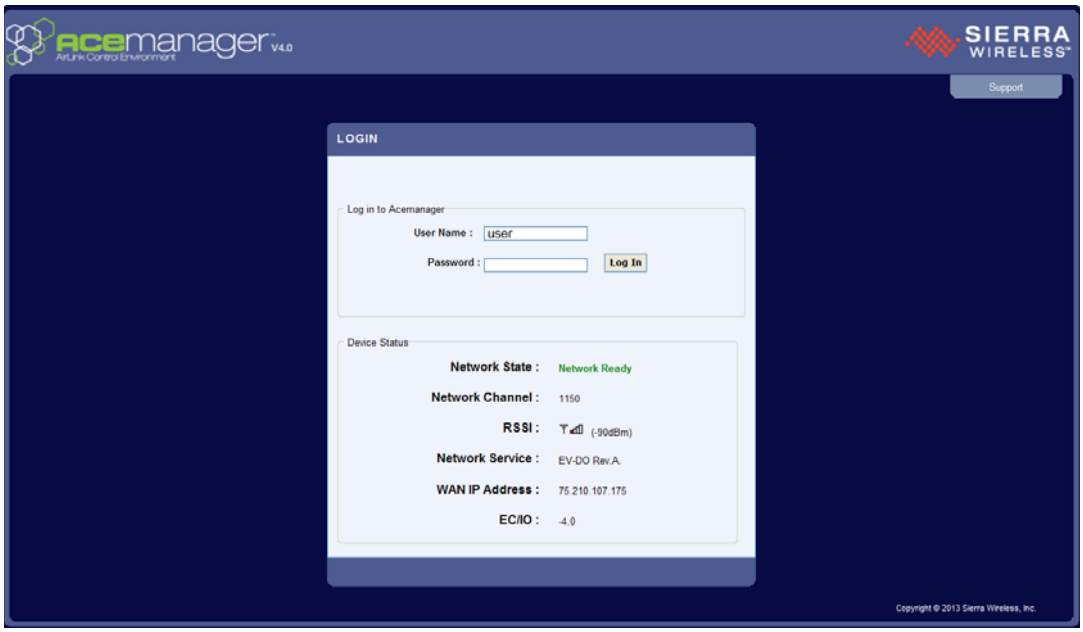


Figure 2-2: ACEmanager: Main Login screen with Device Status

Main Menu Tabs

The main menu for ACEmanager, which appears across the top of the display, is as follows:

- Firmware: Upgrades the ALEOS software
- Upload: Loads configured information, in the form of a template, to the device
- Download: Saves and copies a checked configuration to create a template. If no fields are checked, all fields are selected and saved automatically
- Reboot: Reboots the device
- Refresh All: Refreshes all ACEmanager pages

Configuring

There are two options for configuring the AirLink device:

1. Use the browser based ACEmanager (as detailed in this guide); or
2. Use a terminal emulator application (e.g., Tera Term, PuTTY, etc.) to enter AT commands for many of the configuration options.

Note: Most configuration changes go into effect only after rebooting the AirLink device.

Creating a Template

If you have a device configuration that works well for your needs, you can use ACEmanager to save that device's configuration as a template and then apply it to other Sierra Wireless AirLink devices.

Templates can be created as either feature-specific or for all configurable features. Feature-specific templates are quicker and more reliable to apply from one device to another. Because only specific feature fields are included in the template, all other configuration elements are not altered. This allows for different configurations for particular features not to be overwritten.

To create a template with ACEmanager:

1. Configure your AirLink device in ACEmanager.
2. Click Apply (in the upper right hand corner of the ACEmanager screen) so that the configuration settings write to the device.

Note: When you click the Apply button on any tab, the changes made on all tabs are applied. You do not need to go into the individual tabs to apply changes.

   a. For feature-specific templates, check the boxes in front of the fields to be saved to the template. This allows you to have a template covering only the configuration items you want imported into another device. For tables, click the box at the top of the table to include the entire table.
   b. For templates with all configurable fields, **do not** check any of the boxes.

3. Click Download to save the template. A confirmation dialog box appears.

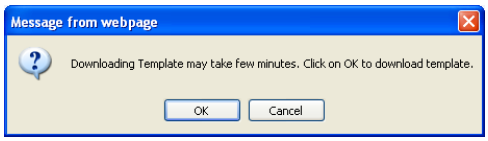


Figure 2-3: ACEmanager: Download Template Message

Note: There is a time delay as the template downloads. A yellow-lit text message of the downloading process appears.

4. Click OK. The File Download box appears.

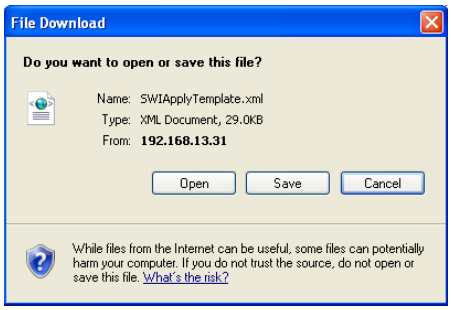

File Download
Do you want to open or save this file?
Name: SWIApplyTemplate.xml
Type: XML Document, 29.0KB
From: 192.168.13.31
Open
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

Figure 2-4: ACEmanager: File Download Box

5. Click Save (or OK depending on your system browser).

Note: Some of the configuration settings are specific to individual devices. Avoid having those settings in your saved template as the devices you configure with the template could cease to work with the cellular or local network. A feature specific template allows you to omit configuration elements which need to be specific to a device.

6. Type in a file name that is descriptive of the template (to easily find it later) and save it to a location on your computer. Not all browsers allow you to change the name of the file while downloading. As long as you do not change the extension .xml, you can change the name and location of the file after it has downloaded.

The template downloads.

Applying a Template

You can use a template you created with the above steps, or a template provided by your AirLink representative or someone in your company who has set up a device template.

You can save the template to:

- Your computer's hard drive and apply it locally (following the instruction below)
- An FTP site and use an AT command to apply the template remotely (for more information, see *TPLUPDATE on page 323).

Note: You can apply templates that contain X-Card information, such as Wi-Fi configuration information, or Dual Ethernet X-Card fields, even when an X-Card is not present in a device. Those fields that do not apply to the device that the template is downloaded to are not displayed.

To apply the template locally to a device:

1. Connect to the device you want to configure using ACEmanager.
2. Click the Upload button on the toolbar.

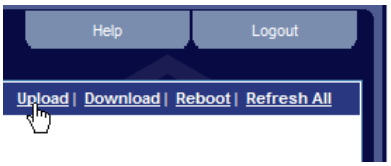


Figure 2-5: ACEmanager: Load

3. At the Upload window, click Browse, and select the template you have saved. You may need to change folders if you saved it to a different location.

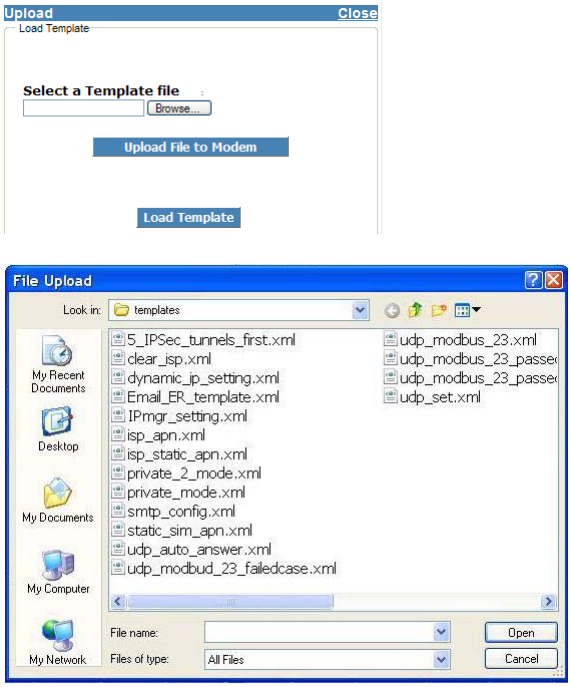


Figure 2-6: ACEmanager: Select and Upload Template

4. Click Upload File to Modem.
5. Click Load Template. As in the template creation process, there is a time delay as the template uploads.

Note: If you are uploading a large template, you may see pop-up windows referring to a script error. This is a time-out error. Retry once or twice before stopping the script and reloading the template.

Tip: *After you load the template, it's best to go back over the ACEmanager tabs to make sure all the settings are what you require. Red asterisks (*) appear on the tabs that have been changed. Make any adjustments to the settings as needed.*

6. Click the Apply button on the toolbar to write the configuration to the device.
7. Click OK.
8. Click the Reboot tab to reset the device.

Caution: *Many configuration settings do not take effect until the device has been reset.*

Tip: *Use the common settings on one device to configure the same settings on another device. For example, use the serial settings on one device to configure these settings on another device.*

AT Command Mode

SSH PAD Mode

SSH PAD mode allows a PAD mode TCP connection to be encrypted using an SSH tunnel and a serial connection to the router or other connected device.

Figure 2-7 shows the network configuration.

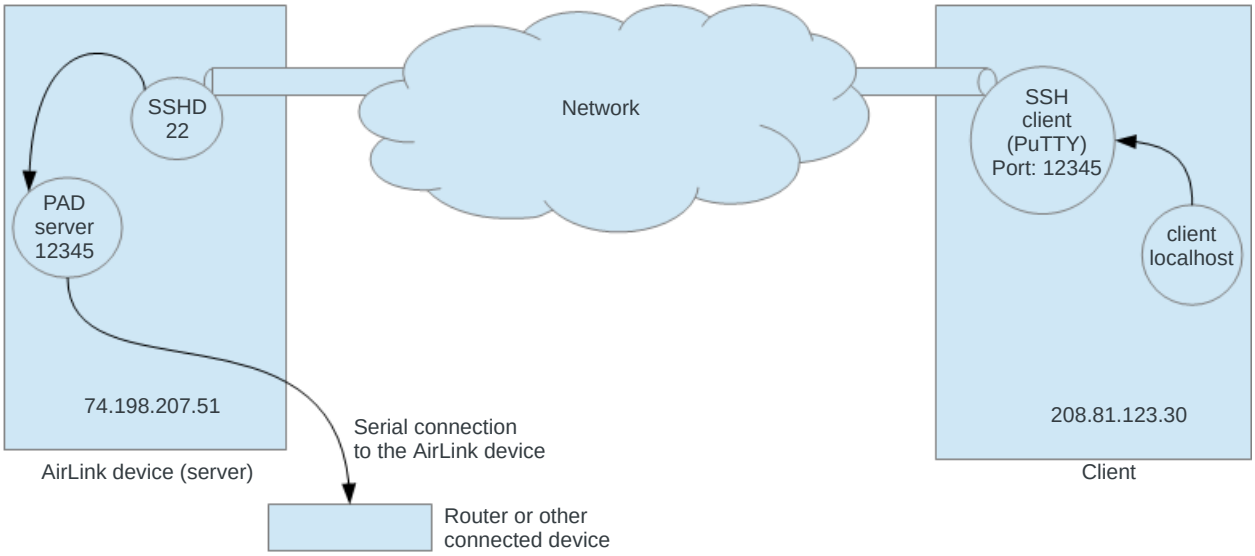


Figure 2-7: SSH Network

Note: For the purpose of illustration, this user guide uses port 12345 on the client, the default port 22 for creating an SSH section, and PuTTY as the SSH client throughout. When configuring SSH PAD mode, you can use any SSH client and values that are appropriate for your network.

The main steps in establishing a secure connection are:

1. Configure an SSH tunnel (on port 12345 in this example) on the client using an SSH client such as PuTTY.
2. Using the SSH client configuration to create the tunnel, log into the AirLink device with the user name and password. The SSH server authenticates the user.
3. The client application that wants to communicate with the PAD server on the AirLink device connects to “localhost” on port 12345.
4. Any data sent on this connection is tagged with a destination port of 12345.
5. The data is received by the SSH server on the AirLink device.
6. The SSH server receives the data with the tag of 12345 and uses port forwarding to send the data to the PAD server.

Server Configuration

You can enable SSH PAD mode on ALEOS by using functionality in the Secure Shell Daemon (SSHD) and by making some changes to the ACEmanager configuration. Currently, tunneled connections can only be initiated by a client that connects to the server on ALEOS.

Enabling SSH

The SSH Daemon must be running on the AirLink device. To enable it:

1. In ACEmanager, go to Services > Telnet/SSH, and in the Remote Login Server Mode drop-down menu, select SSH.
2. In the Remote Login Server Telnet/SSH Port field, enter the desired port number (or use the default SSH port 22).

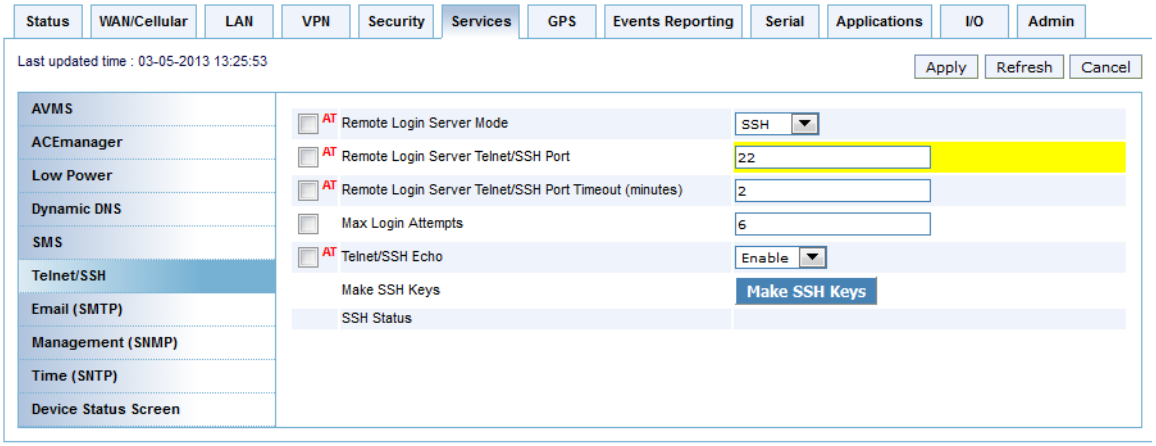


Figure 2-8: ACEmanager: Services > Telnet/SSH

3. Click Apply.

Enabling PAD Mode

ALEOS uses PAD mode to accept TCP connections. To enable PAD mode:

1. In ACEmanager, go to Serial > Port Configuration.
2. Set DB9 Serial Echo to Disable.
3. Set the Device Port field to the desired value (12345 in this example).
4. Set the destination Address to the IP address of the client that will be connecting to the AirLink device in SSH PAD mode.
5. Under Advanced, set Quiet Mode to Enable.
6. Under TCP, set TCP Auto Answer to Enable.

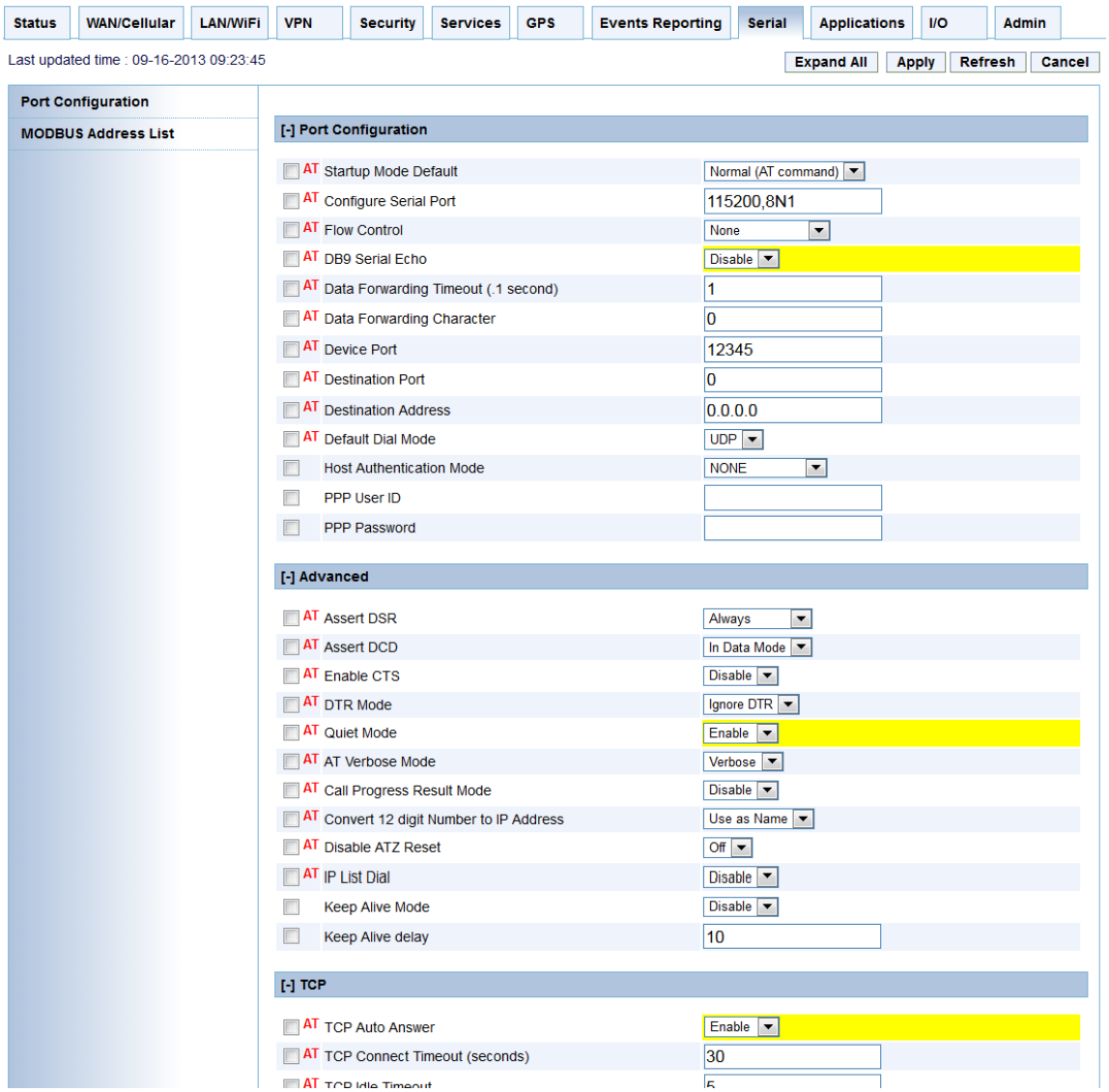


Figure 2-9: ACEmanager: Serial > Port Configuration

7. Click Apply.

Client Configuration

Creating Client Tunnel

Configure the SSH client to create a tunnel when it connects to the AirLink device. (In this example, PuTTY is used to create the tunnel.)

1. Create a new SSH session by entering the IP address of the AirLink device, and the configured port. (In this example, the IP Address of the AirLink device is 74.198.207.51 and default port 22 is used.)

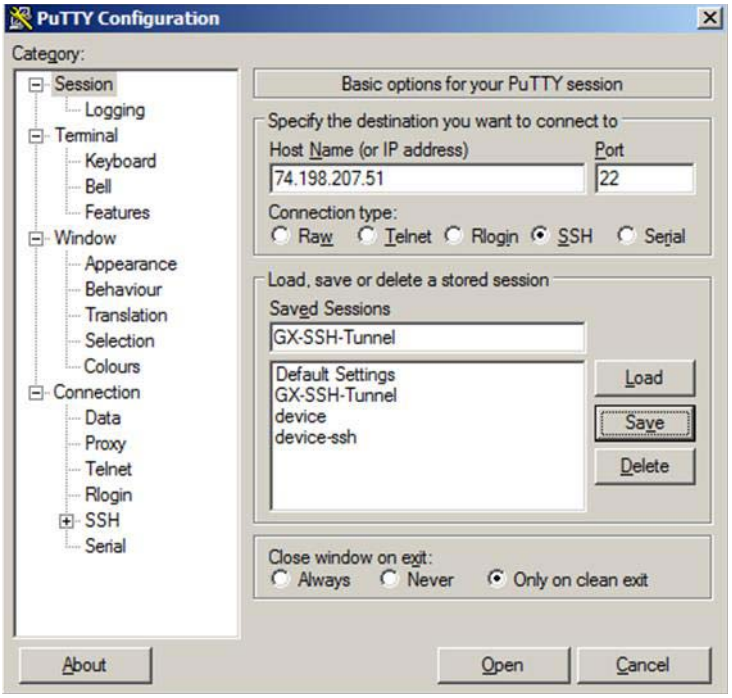


Figure 2-10: PuTTY: Creating a new SSH session

2. Click Save.
3. Go to Connection > SSH > Tunnels.
4. Create an SSH tunnel for the connection by creating a forwarded port.

   In the Source port field, enter the same value as the Device Port field configured in ACEmanager Serial port configuration (12345 in this example). This is the port that the PAD session listens on for incoming connections.

   In the Destination address field, enter the IP address of the AirLink device. (You can find this in ACEmanager on the Status > Home page.) The port is also listening to the TCP port for PAD mode (Device Port on the Serial tab) which, in this example, is 12345.

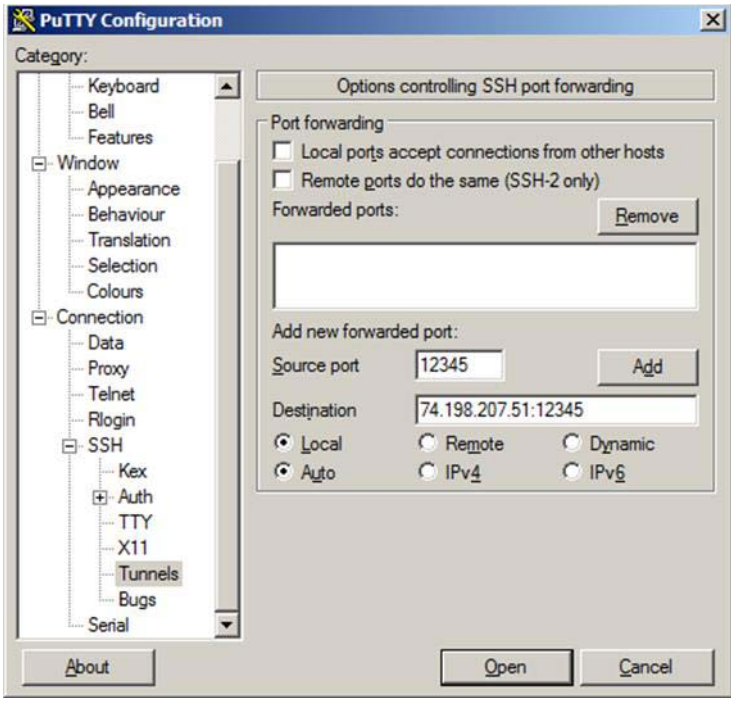


Figure 2-11: PuTTY: Creating an SSH tunnel

5. Leave the Local and Auto settings selected.

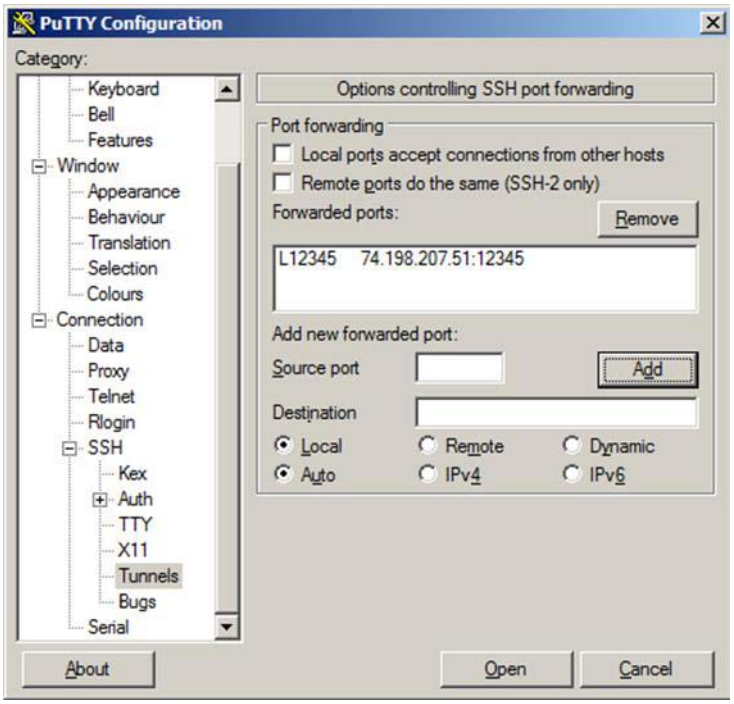


Figure 2-12: PuTTY: SSH tunnel created

6. Click Add.
7. Go to Connection > SSH.

8. Under Protocol options, select “Don’t start a shell or command at all” to prevent getting a command prompt.

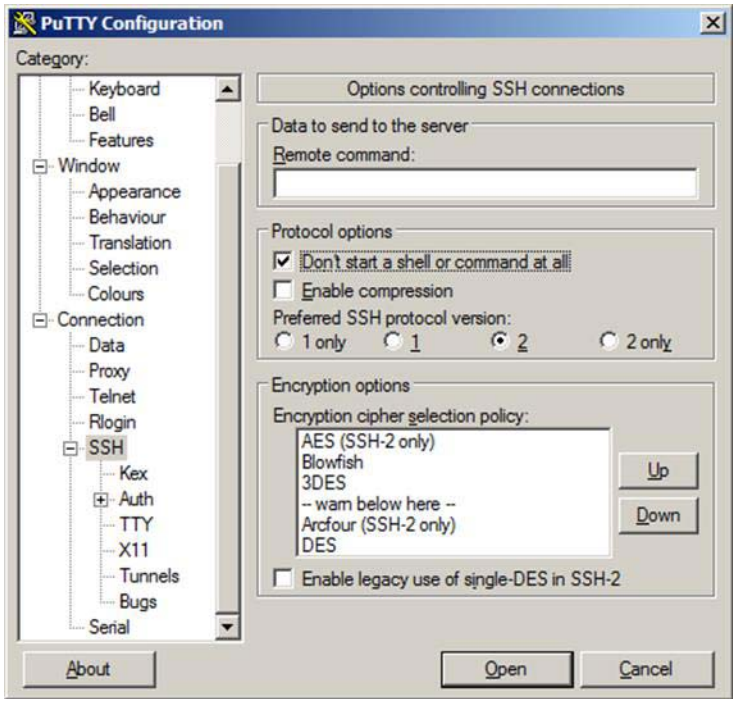


Figure 2-13: PuTTY: SSH Connection Settings

9. Click Open to create a connection to the AirLink device. Log in with the user account.
10. With the client application, establish a TCP connection to localhost using the configured port. (In this example, 12345.)

Important: *If you connect to the IP address of the AirLink device (74.198.207.51) instead of localhost, the tunnel is bypassed and the data is unencrypted.*

All data transmitted to the AirLink device should now be encrypted.

Update the ALEOS Software and Radio Module Firmware

To take advantage of new features available in the latest version of ALEOS, update the ALEOS software and radio module firmware on your AirLink devices.

You can use ACEmanager to update one device at a time or AVMS to update one or multiple devices at the same time.

Step 1—Planning Your Update

1. For each of the devices you want to update, make a note of the:
   - Device Model
   - Radio Module Type
   - Radio Firmware Version
   - ALEOS Software Version
   - Mobile Network Operator

   Information for the first four bullets is available in AVMS and in ACEmanager (Status > About). The ACEmanager Status > Home screen shows the Mobile Network Operator.

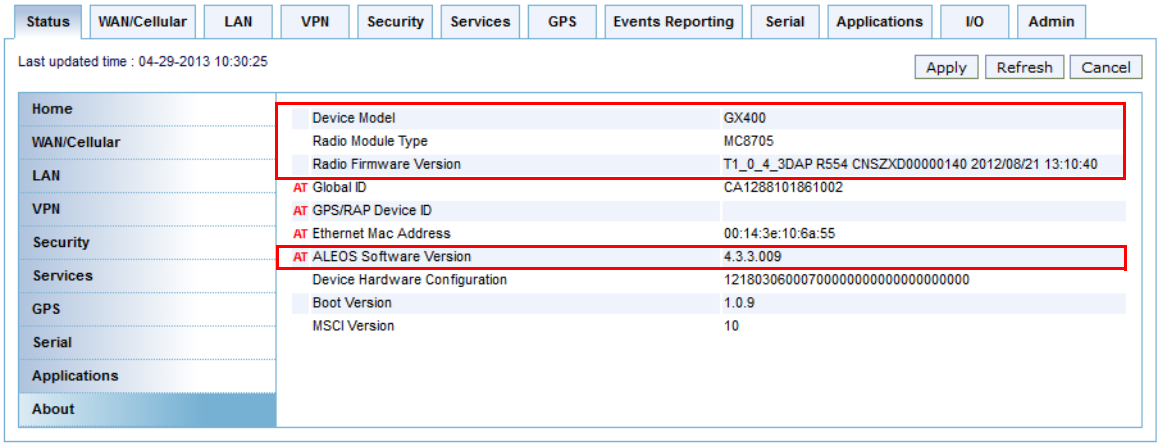


Figure 2-14: ACEmanager: Status > About

2. Refer to Table 2-1 and Table 2-2 on page 29 for the supported upgrades for your device.

Table 2-1: GX Series Radio Module Firmware Supported with ALEOS[a]

Radio Module Type	Current Radio Firmware Version	ALEOS version:		
		4.3.3	4.3.3a	4.3.4
MC5728	p2813301	✔	X	X
Verizon GX400 MC5728	p2815600	✔	✔	✔

Table 2-1: GX Series Radio Module Firmware Supported with ALEOS[a] (Continued)

Radio Module Type	Current Radio Firmware Version	ALEOS version:		
		4.3.3	4.3.3a	4.3.4
MC7700	SWI9200X_03.05.10.02AP R4684 CARMD-EN-10527 2012/02/25 11:58:38	✔	✔	✔
	SWI9200X_03.05.14.00AP R5164 CARMD-EN-10527 2012/05/29 19:13:25	✔	✔	✔
MC7750	SWI9600M_01.00.09.03AP R2492 CARMD-EN-10526 2011/07/01	X	X	X
	SWI9600M_03.05.10.06ap r5595 carmd-en-10527 2012/11/12	✔	✔	X
	SWI9600M_03.05.10.09ap r5700 carmd-en-10527 2013/03/12 10:37:48	X	X	✔
MC8705	T1_0_3_2AP R361 CNSZXD00000061 2011/04/15 17:40:48	✔	✔	✔
	T1_0_4_3DAP R554 CNSZXD00000140 2012/08/21 13:10:40	✔	✔	✔
	T3_5_3_2AP R551 CNSZXD00000140 2012/06/05 18:03:33	✔	✔	✔
	T1_0_4_3CAP R460 CNSZXD00000128 2011/11/15 10:22:30	X	X	X

a. ✔ = Supported
X = Not Supported. When updating the device, you will be prompted to use the supported radio module firmware.

Table 2-2: LS300 Radio Module Firmware Supported with ALEOS[a]

Radio Module Type	Current Radio Firmware Version	ALEOS version:		
		4.3.3	4.3.3a	4.3.4
SL5011	p3110506	✔	✔	✔
	p3110503	✔	✔	✔
SL8090	P1_0_0_8AP R1338 CNHKGDKCE01 2011/10/21 09:21:31	✔	✔	✔
SL8092	P1_0_0_8AP R1338 CNHKGDKCE01 2011/10/21 09:21:31	✔	✔	✔

a. ✔ = Supported
X = Not supported. When updating the device, you will be prompted to use the supported radio module firmware.

3. Refer to the flowchart (Figure 2-15 on page 30) to determine the ALEOS software required.
4. If you are planning to use ACEmanager to do the update:
   a. Go to www.sierrawireless.com/Support/Downloads.aspx and select your product and mobile network operator to get to the download page for your device.
   b. Download the new ALEOS software version for your system. If new Radio Module firmware is required for this product, it will be included with the ALEOS Software in a .zip file.

If you have any questions or concerns, contact Sierra Wireless Support. (See Contact Information on page 4.)

ALEOS Software and Radio Module Firmware Update Overview

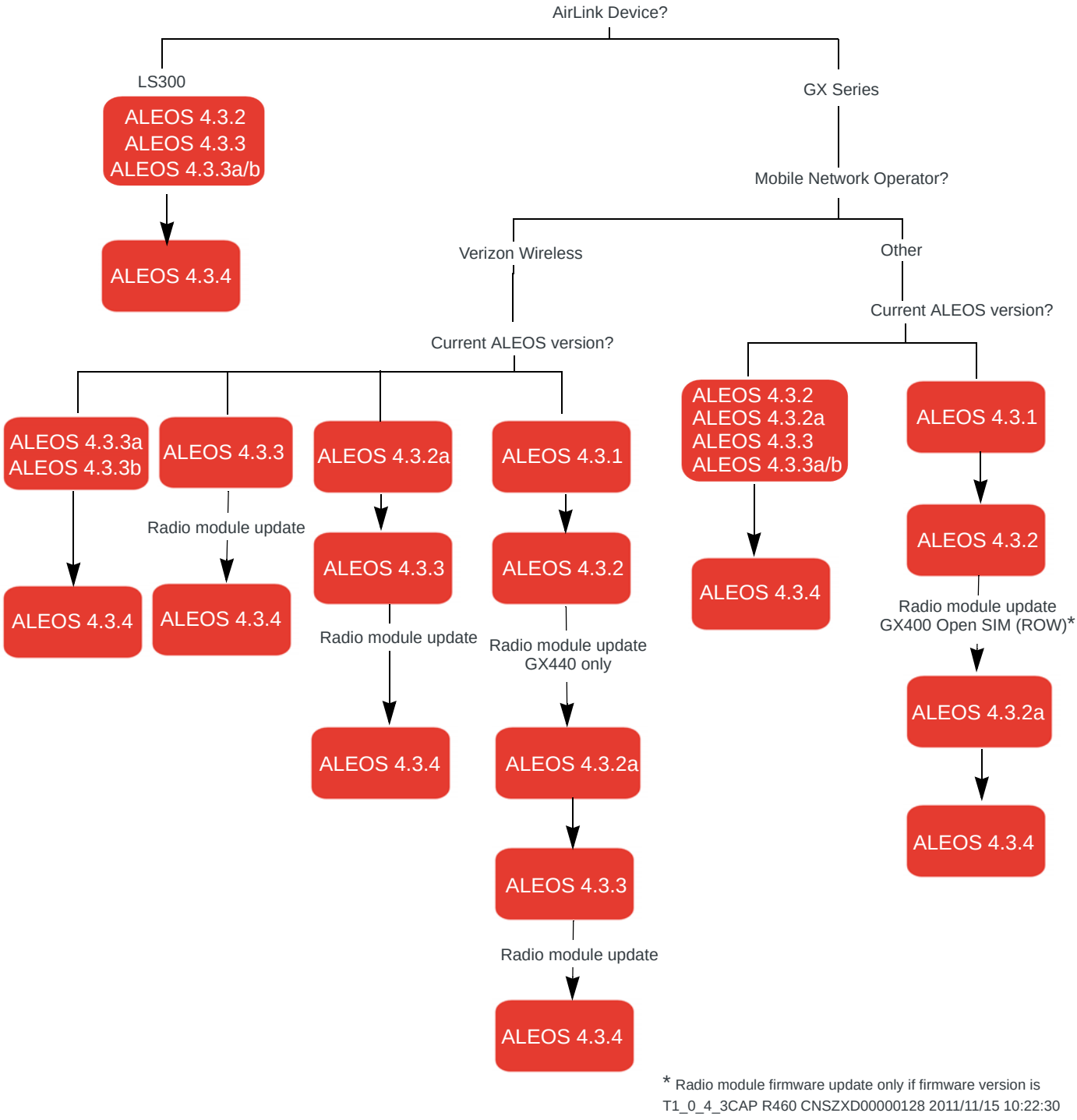


Figure 2-15: ALEOS software update overview

Recommendations

Sierra Wireless recommends that you contact your authorized Sierra Wireless distributor before updating the radio module firmware.

Scheduling the update

The update can take up to 30 minutes to complete, depending on the speed of your network connection. The AirLink device being updated will be off-line during the update, so take this into account when scheduling the update.

Important: *BE PATIENT! The firmware update can take up to 30 minutes to complete. Ignore connection time out messages—the update process is still running.*

Waiting for the process to complete is faster than troubleshooting the problems that can be caused by interrupting the process midway. (Interrupting the process may result in having to return the device to the factory for repairs.)

Step 2—Update the ALEOS Software and Radio Module Firmware

Using ACEmanager to Update a Single AirLink Device

To update the ALEOS software and radio module firmware on one AirLink device:

1. Connect the AirLink device you want to upgrade to your laptop, launch your browser and enter the URL for the device. The default IP address for the Ethernet interface is http://192.168.13.31:9191. If it is a remote device, enter the domain name or public IP (WAN) address.

Note: If you are connected to the device remotely, any files transferred to the device are transferred over-the-air and you may incur data charges. (For file size information, see the flowchart on page 30.)

2. Log in to ACEmanager.
   User name: user
   Default password: 12345
3. Click the Firmware link.
   The Firmware Update window opens.

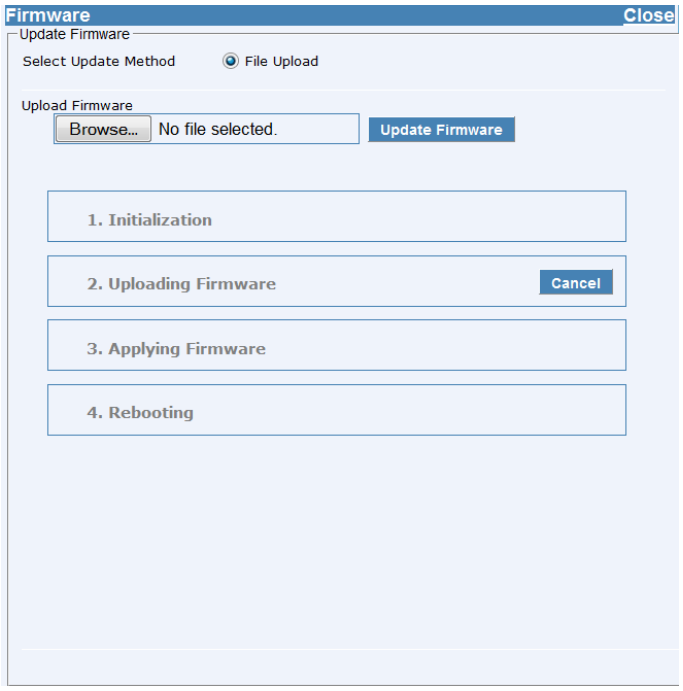


Figure 2-16: Firmware Update window

If you are updating from ALEOS 4.3.4 to 4.3.4-I, the update window shows the current ALEOS and radio module firmware versions and the device model. It also gives you the option to update both ALEOS and the radio module firmware, or update only the radio module firmware. Unless advised otherwise by Sierra Wireless, we recommend that you select ALEOS software (which updates ALEOS and prompts you to update the radio module firmware if a newer version is available for your device).

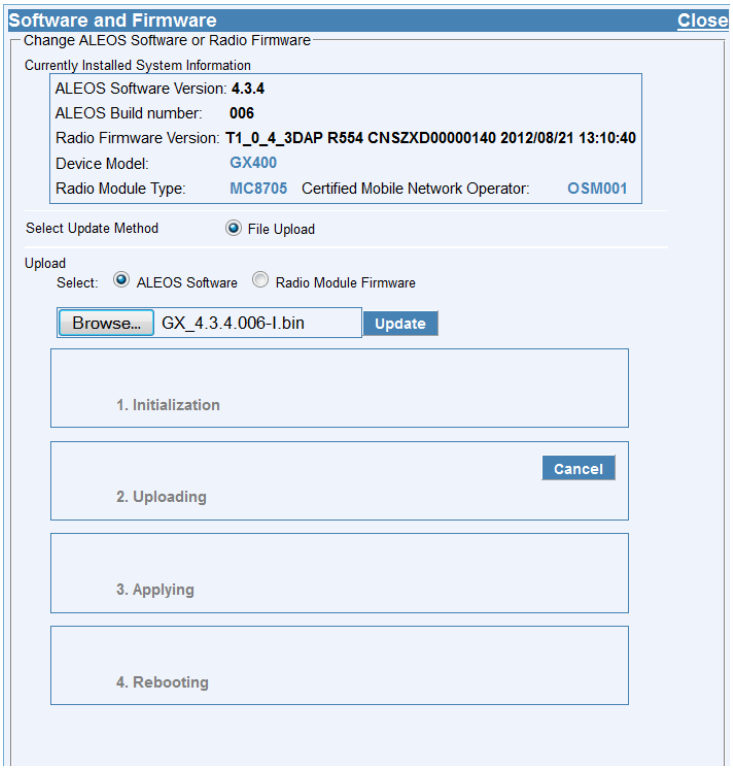
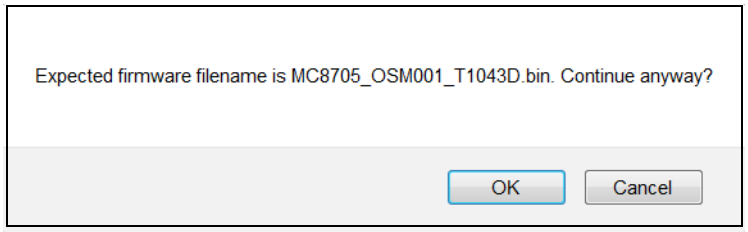


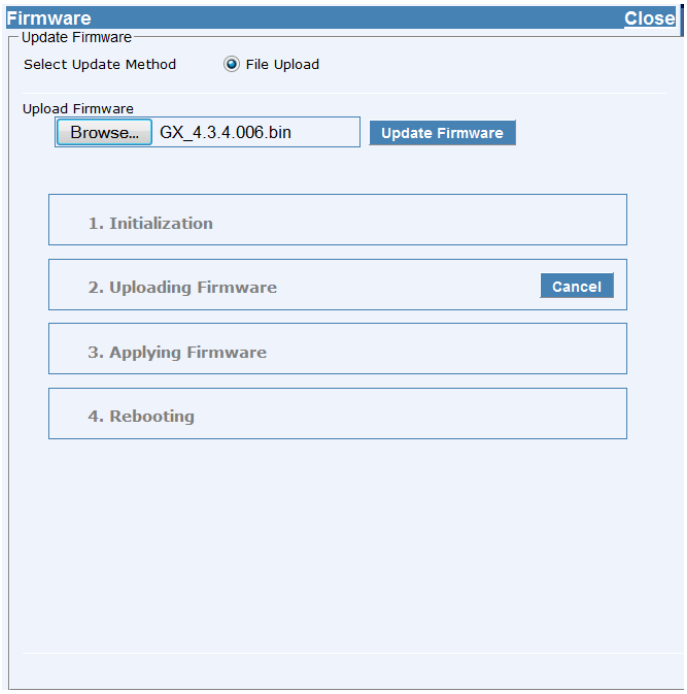
Figure 2-17: ALEOS 4.3.4 Software and Firmware update window

4. Click Browse... and navigate to the ALEOS software you downloaded from the Sierra Wireless Web site.

   If you select a file that is not supported on your device, you will see a warning message similar to the following:



   Unless you have been advised by Sierra Wireless to do so, we recommend you do not install an unsupported version of the radio module firmware. For a list of supported radio module firmware files for your device, see Table 2-1 on page 28 and Table 2-2 on page 29.



5. Click Update Firmware.

   The ALEOS software update runs automatically and green check marks appear beside each step, as it is completed. If you are doing the upgrade over-the-air (especially if you are doing a radio module update), it may occasionally appear as if the next step is beginning before the green check mark appears. This is a known issue in the UI and does not affect the update.

Figure 2-18: ALEOS software update in progress

Important: *Do not disconnect the AirLink device from the computer, and do not power cycle or reset the device during the update. If you see any error messages, refer to the* *Updating the ALEOS Software and Radio Module Firmware on page 386.*

6. Depending on the version of ALEOS you are updating to, ALEOS may check the radio module firmware and prompt you if it needs to be updated.

   If you do not receive a prompt, the radio firmware is up to date. Proceed to step 9.

   If you are prompted to update the firmware, proceed to step 7.

7. Under Applying Firmware, click Browse... and navigate to the radio module firmware you downloaded from the Sierra Wireless Web site.

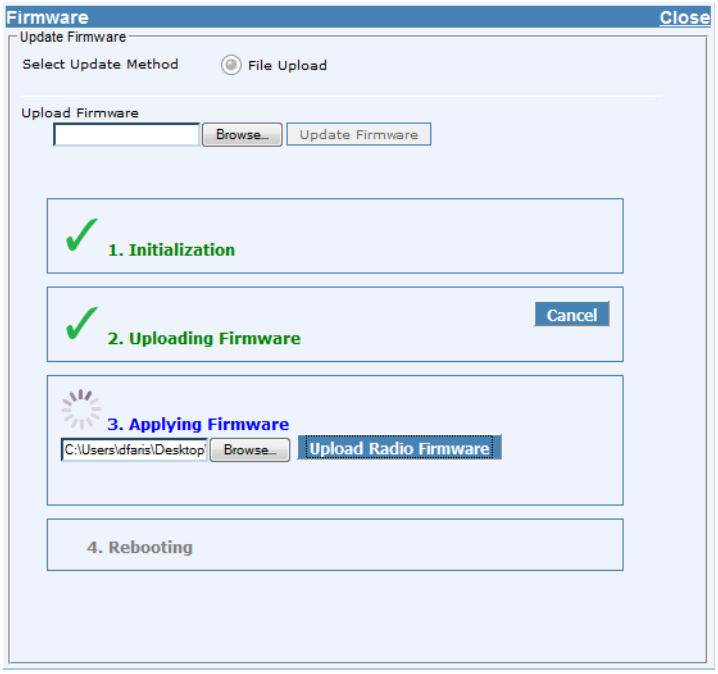
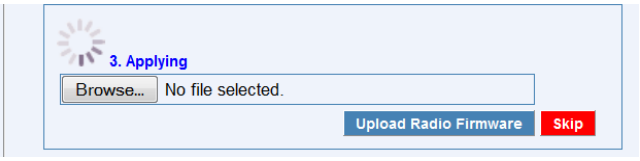
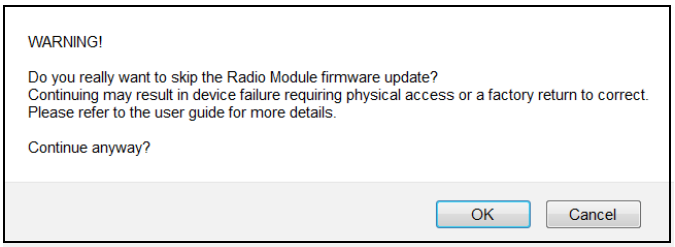


Figure 2-19: ALEOS software update in progress, prompt to update radio module firmware

If you are updating from ALEOS 4.3.4 to 4.3.4-I, you may be given the option to skip the radio module firmware.



We recommend that you do NOT skip the radio module firmware update unless advised to do so by Sierra Wireless. If you choose to skip the radio module firmware update, you'll see the following warning.


WARNING!
Do you really want to skip the Radio Module firmware update?
Continuing may result in device failure requiring physical access or a factory return to correct.
Please refer to the user guide for more details.
Continue anyway?
OK
Cancel

8. Click Upload Radio Firmware.

   The radio module firmware may take 10 to 20 minutes to upload and install.

Important: *Do not disconnect the AirLink device from the computer or reboot the device while the firmware update is in progress. During the radio module firmware update, the device LEDs flash rapidly in sequence (an LED chase or caterpillar). When the radio module firmware update is complete, the device reboots automatically.*

If you see a message saying that the connection has timed out, ignore the message and continue to wait for the device to reboot.

If you clicked OK when you saw the timed out message and logged back in, you'll see the old version of the firmware. The firmware update process is still going on, so DO NOT reset the device or disconnect the power. DO NOT click Cancel. Continue to wait the 10 to 20 minutes for the radio module firmware update to complete. The device reboots once the firmware update is complete.

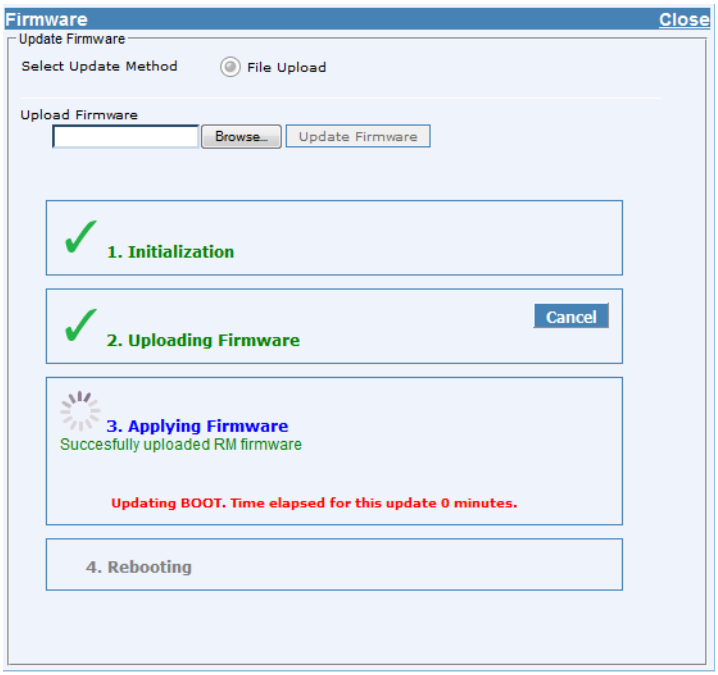


Figure 2-20: Radio module firmware update in progress

9. When the update is complete, the AirLink device reboots and you are returned to the Login screen.

10. When you see the Login screen, wait a few seconds to ensure that the reboot is complete and then log in.
11. Go to Status > About.
12. Click Refresh. Once the device has an IP address, check the ALEOS Software Version and the Radio Firmware Version fields to confirm that the ALEOS software and the radio module firmware have been updated.

    If the ALEOS software version and the radio module firmware version have not been updated, repeat the firmware update.

Using AirVantage Management Service (AVMS) to Update One or Multiple AirLink Devices Over-the-Air

You can use AirVantage Management Service to update the ALEOS software and radio module firmware over-the-air on one or multiple AirLink devices.

If you don't have an AVMS account:

1. In ACEmanager, go to the Services tab and ensure that AVMS is enabled and the server URL is http://na.m2mop.net/msci/com. If this is not the case, enter the correct URL, click Apply and then click Reboot.
2. Go to www.sierrawireless.com/en/productsandservices/AirVantage/Management_Service.aspx for more information. To sign up for a free trial account, go to http://na.airvantage.net.

Updating to ALEOS software with an AVMS account:

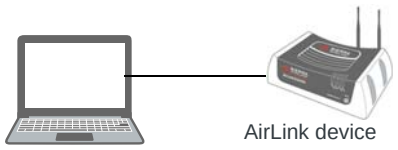
3. Go to http://na.airvantage.net/start and log in.
4. Follow the instructions in the online AVMS documentation to update the ALEOS software and radio module firmware.

Enterprise LAN Management

You can use AirLink devices in the following configurations:

- Standalone with a connection to a single host

  When using the AirLink device with a single host, ensure that the host is DHCP enabled.



- With a router

  The router allows several hosts to use the AirLink device's connection to the network. When using the AirLink device with a router:

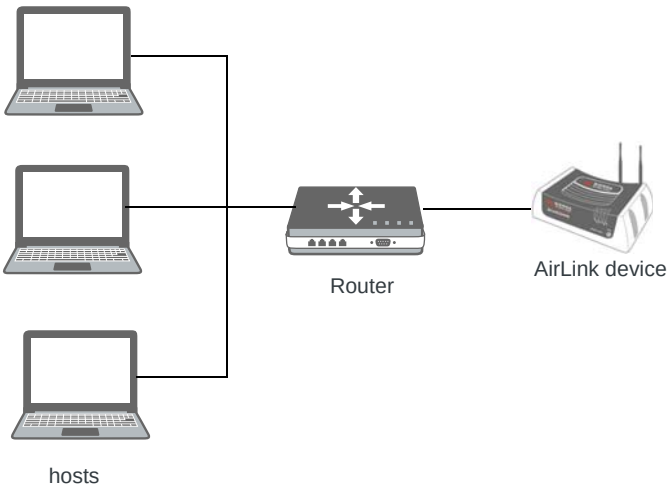
  · Configure the router to be DHCP enabled.

  And either:

  · Configure the router to use Network Address Translation (NAT).

  Or

- Configure ALEOS (in ACEmanager) to use Host Port Routing. For information on using ALEOS with a router that is not configured to use NAT, see Host Port Routing on page 84.



Note: Other than for VLANs, ALEOS does not provide DHCP addresses to router connected hosts.

Over the Air (OTA) Connections

Access AirLink devices

You can use an OTA connection to access AirLink devices that are in either configuration described above (stand alone or with a router).

Access connected hosts

To use an OTA connection to access a connected host through the AirLink device, configure the host in ALEOS as the DMZ or port forwarding destination. For information on inbound OTA connections to the host, see DMZ on page 137 and Port Forwarding on page 133.

Configuring Your Device for use in a PCI Compliant System

The credit card industry requires retailers to comply with Payment Card Industry (PCI) standard to maintain a secure environment when processing payment card transactions. For these transactions, the AirLink ES440 acts as a wireless data conduit for routers and PoSs (point-of-sale-terminals) that have been configured for PCI compliance.

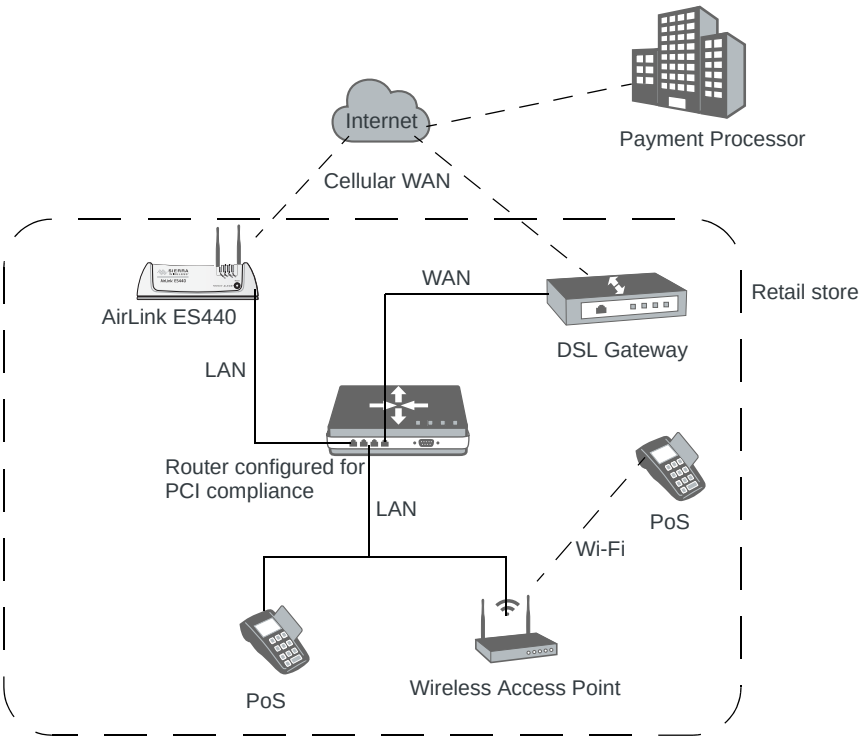


Figure 2-21: Sample PCI compliant network

The PCI compliant network must be set up so that:

- The USBnet is on a different subnet from the point-of-sale-terminal.
- All security protocols must be established from the point-of-sale terminal to the payment processor.
- Payment card terminals must be on a dedicated LAN or VLAN.
- The AirLink device must be connected to a router that is configured for PCI compliance.

Note: The serial port on the AirLink device has no access to the IP data path and does not need to be disabled.

If you are using the AirLink ES440 for a payment card industry application, to meet PCI Data Security Standard compliance requirements the following steps must be done by a PCI certified service company.

For each device:

1. Connect the AirLink device to a router that has been configured for PCI compliance.
2. Log in to ACEmanager. (User name is user; default password is 12345.)
   Change the password regularly, in accordance with PCI recommendations.
3. Go to the Admin tab and change the default password.
   Do not share the ACEmanager password.
4. Go to Applications > ALEOS Application Framework and set the ALEOS Application Framework field to Disable.

3: Status

All of the fields in the “Status” group are read-only and provide information about the AirLink device. Depending on the individual settings and the onboard cellular module of the AirLink device, the actual status pages may look different than the screen shots shown here. The individual status sections give an accurate view of the current running configuration of the AirLink device. Refer to the following sections for information about the individual configuration options.

Home

The Home section of the Status tab is the first page displayed when you login to ACEmanager. It shows basic information about the cellular network connection and important information about the device.

Tip: *See WAN/Cellular Configuration on page 103 for information about configuring the cellular settings.*

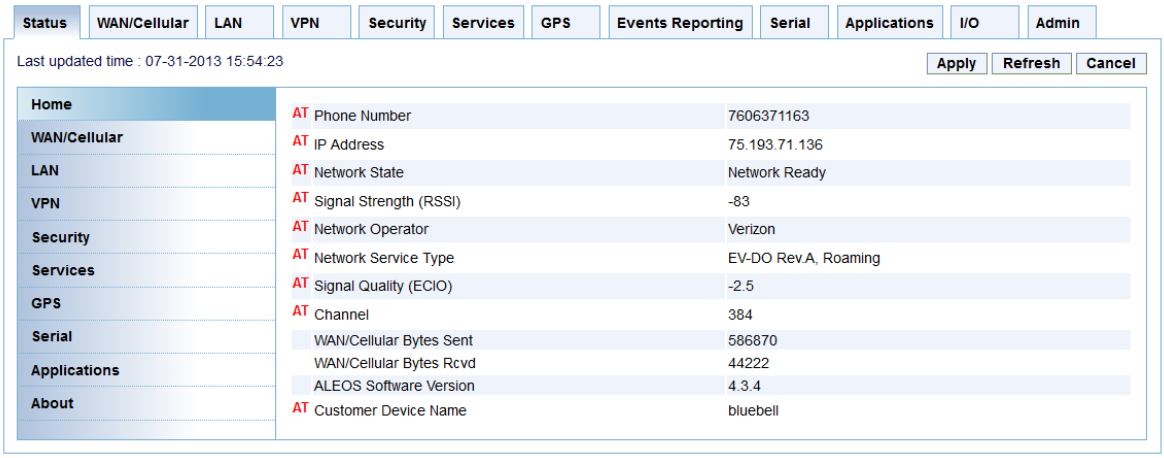


Figure 3-1: ACEmanager: Status > Home — CDMA

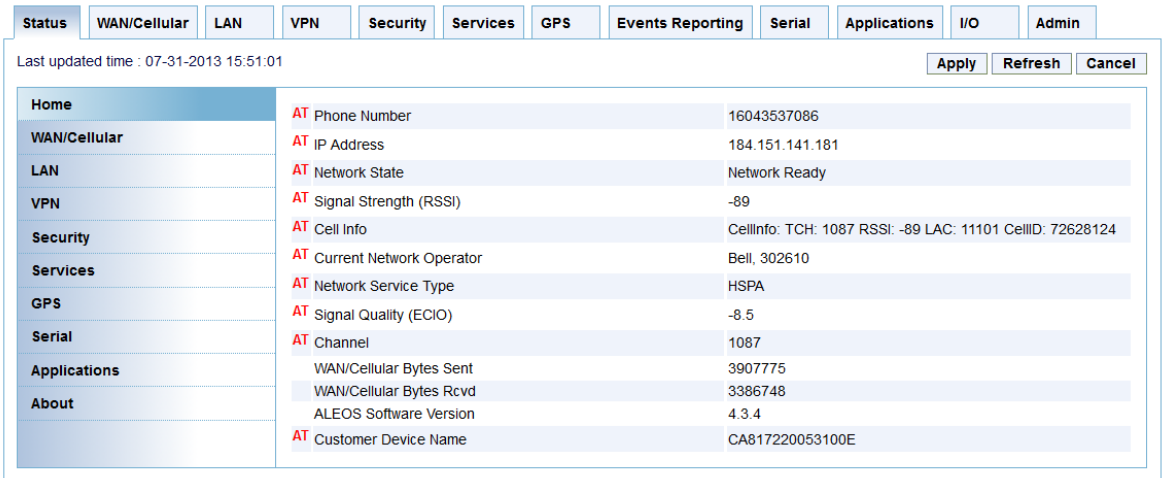


Figure 3-2: ACEmanager: Status > Home — HSPA

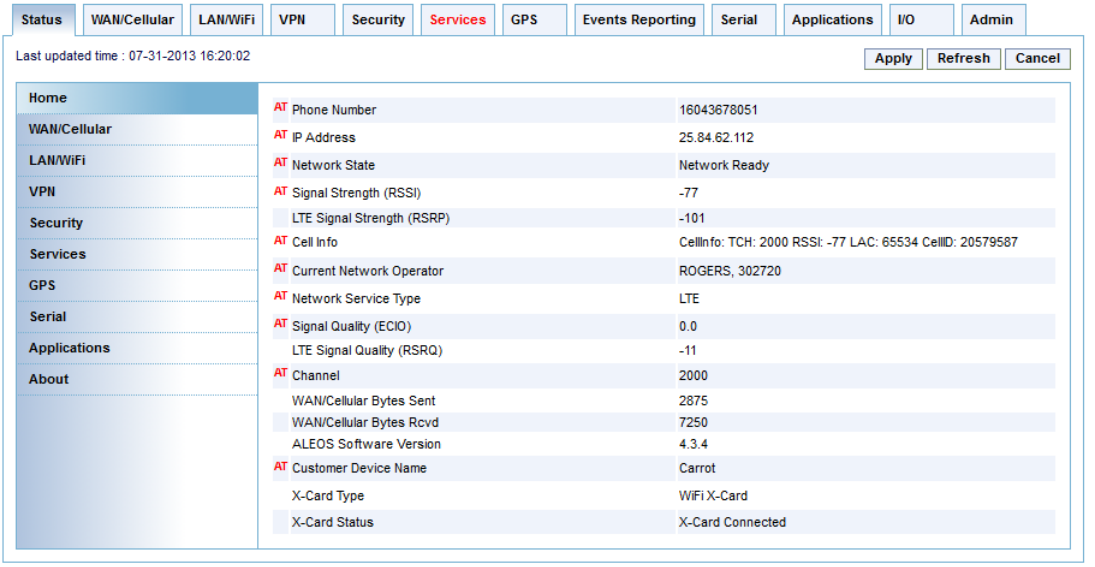


Figure 3-3: ACEmanager: Status > Home — LTE

Field	Description
Phone Number	The phone number (programmed into the device) associated with the Mobile Network Operator account
IP Address	The current WAN IP address for the device. This can be the IP address for either a Wi-Fi or cellular interface. If both these interfaces have valid IP addresses, the IP address used by Wi-Fi is shown.

Network State	Current state of the cellular radio network connection • Network Ready—Connected to a mobile broadband network and ready to transfer data • Network Ready WiFi—Connected to a Wi-Fi network and ready to transfer data • Connecting To Network—Establishing a network connection; wait until the connection is established • Connecting To Network - WiFi—Establishing a connection to a Wi-Fi network; wait until the connection is established • Data connection failed. Waiting to retry—ALEOS is attempting to reconnect to the mobile broadband network. Ensure that the APN is correct or the account is activated to the ESN for your device. Wait until it is able to connect. If you see this status repeatedly or for an extended period of time, contact your Mobile Network Operator. • Network Link Down—Unable to connect to the network. Ensure that the APN is correct or the account is activated to the ESN for your device. If the problem persists, contact your Mobile Network Operator. • Network Link Down - WiFi—Unable to connect to the Wi-Fi access point. Check the authentication information. • No SIM or Unexpected SIM Status—Unable to read the SIM information; check that the SIM card is installed correctly. • SIM PIN incorrect x attempts left—Wrong SIM PIN entered; enter the correct PIN. If the correct PIN is not entered in the specified number of attempts, the SIM is blocked. Contact your Mobile Network Operator to unblock the SIM. • No Service—Unable to connect to the broadband network. Check that the antenna is connected properly. If the problem persists, contact your Mobile Network Operator for information about coverage in your region. • Provisioning...—(CDMA networks only) The Mobile Network Operator is updating the radio module firmware with your account details. Wait until the provisioning is complete. • Awaiting provisioning...—(CDMA networks only) The device does not yet have an account associated with the radio module and is attempting to contact the Mobile Network Operator to obtain account information. If this state persists, check that the account is activated to the device's ESN. • Starting OMADM state—The Mobile Network Operator is starting an over-the-air (OTA) radio module device management session. Wait until the OTA management session is complete. • In NI PRL Update—(CDMA networks only) An updated Preferred Roaming List is being downloaded from the network. Wait until the download is complete. • NI PRL Failed—(CDMA networks only) The network initiated attempt to update the Preferred Roaming List failed. If the problem persists, contact your Mobile Network Operator. • NI PRL Failed. Waiting to retry—(CDMA networks only) The network initiated attempt to update the Preferred Roaming List failed. The network is waiting to retry the download. Wait until the download is complete. • Network Authentication Failed—Unable to connect to the network because of invalid authentication data. If the problem persists, contact your Mobile Network Operator.

<table>
<tr><td>Signal Strength (RSSI)</td><td>Received Signal Strength Indicator
The averaged received signal power measured in the air interface channel
Indicates if there is a strong signal available for my device to connect to
See also LTE Signal Strength (RSRP) and LTE Signal Quality (RSRQ).
The value varies, depending on the network characteristics and the AirLink device.
<table><tr><th>RSSI</th><th>Signal strength</th></tr><tr><td>> -70 dBm</td><td>Excellent</td></tr><tr><td>-70 dBm to -85 dBm</td><td>Good</td></tr><tr><td>-86 dBm to -100 dBm</td><td>Fair</td></tr><tr><td>< -100 dBm</td><td>Poor</td></tr></table></td></tr>
<tr><td>LTE Signal Strength (RSRP)</td><td>Reference Signal Received Power
The average signal power of all cell-specific reference signals within the LTE channel
Indicates whether the AirLink device has a strong connection to the wireless network
The value varies, depending on the network characteristics and the AirLink device.
<table><tr><th>RSRP</th><th>Signal strength</th></tr><tr><td>> -90 dBm</td><td>Excellent</td></tr><tr><td>-90 dBm to -105 dBm</td><td>Good</td></tr><tr><td>-106 dBm to -120 dBm</td><td>Fair</td></tr><tr><td>< -120 dBm</td><td>Poor</td></tr></table>See also LTE Signal Quality (RSRQ) and Signal Strength (RSSI).</td></tr>
<tr><td>Cell Info</td><td>Provides cell information such as the Base Station Identity Code (BSIC), TCH, Received Signal Strength Indicator (RSSI), Location Area Code (LAC), and the cell ID
For additional information, including cell info for LTE networks, see *CELLINFO2? on page 323.</td></tr>
<tr><td>Current Network Operator</td><td>Provides the name of the Mobile Network Operator whose network the AirLink device is connected to.

Note: The roaming operator is only displayed if the home operator allows this.</td></tr>
<tr><td>Network Service Type</td><td>The type of service being used by the device. Options are:
EV-DO Rev A, 1x, LTE, HSPA+, HSPA, HSDPA, HSUPA, UMTS, EDGE, or GPRS
If you are connected to a network other than that of your Mobile Network Operator, the network service type indicates that you are roaming (and additional charges may apply).</td></tr>
</table>

<table>
<tr><td>Signal Quality (EC/IO)</td><td>CDMA/UMTS signal quality
Indicates the signal quality with a ratio of the average signal energy to co-channel interference in dB
<table><tr><th>EC/IO</th><th>Signal quality</th></tr><tr><td>0 to -6</td><td>Excellent</td></tr><tr><td>-7 to -10</td><td>Good</td></tr><tr><td>-11 to -20</td><td>Fair to Poor</td></tr></table></td></tr>
<tr><td>LTE Signal Quality (RSRQ)</td><td>Reference Signal Received Quality
The RSRQ indicates the quality of the AirLink device’s connection to the wireless network. (Is noise or interference affecting the quality of the connection?) See also Signal Strength (RSSI) and LTE Signal Strength (RSRP).
The value varies, depending on the network characteristics and the AirLink device.
<table><tr><th>RSRQ</th><th>Signal quality</th></tr><tr><td>> -9 dB</td><td>Excellent</td></tr><tr><td>-9 dB to -12 dB</td><td>Good</td></tr><tr><td>< -13 dB</td><td>Fair to Poor</td></tr></table>
Note: For additional information on the LTE network, use the *CELLINFO2? AT command (described on page 323).</td></tr>
<tr><td>Channel</td><td>The CDMA/UMTS channel
The current active channel number that the AirLink device is communication to the network on.</td></tr>
<tr><td>WAN/Cellular Bytes Sent</td><td>Number of bytes sent to the network since system startup or reboot</td></tr>
<tr><td>WAN/Cellular Bytes Rcvd</td><td>Number of bytes received from the network since system startup</td></tr>
<tr><td>ALEOS Software Version</td><td>Version of ALEOS software currently installed in the device</td></tr>
<tr><td>Customer Device Name</td><td>Name of the device as it is configured with the Dynamic DNS IP Manager settings</td></tr>
</table>

X-Card Type	Indicates whether the AirLink device has a connected X-Card or not Values are: • x-Card Not Found • WiFi x-Card • Dual Ethernet x-Card • IO x-Card *Note: This field applies only to the AirLink GX Series devices.*
X-Card Status	Indicates the status of the X-Card, if present Values are: • x-Card Connected • x-Card Disconnected *Note: This field applies only to the AirLink GX Series devices.*

WAN/Cellular

WAN/Cellular provides specific information about the cellular connection including IP address and how much data has been transmitted or received. Some of the information on this page is repeated on the Home page for quick reference.

CDMA

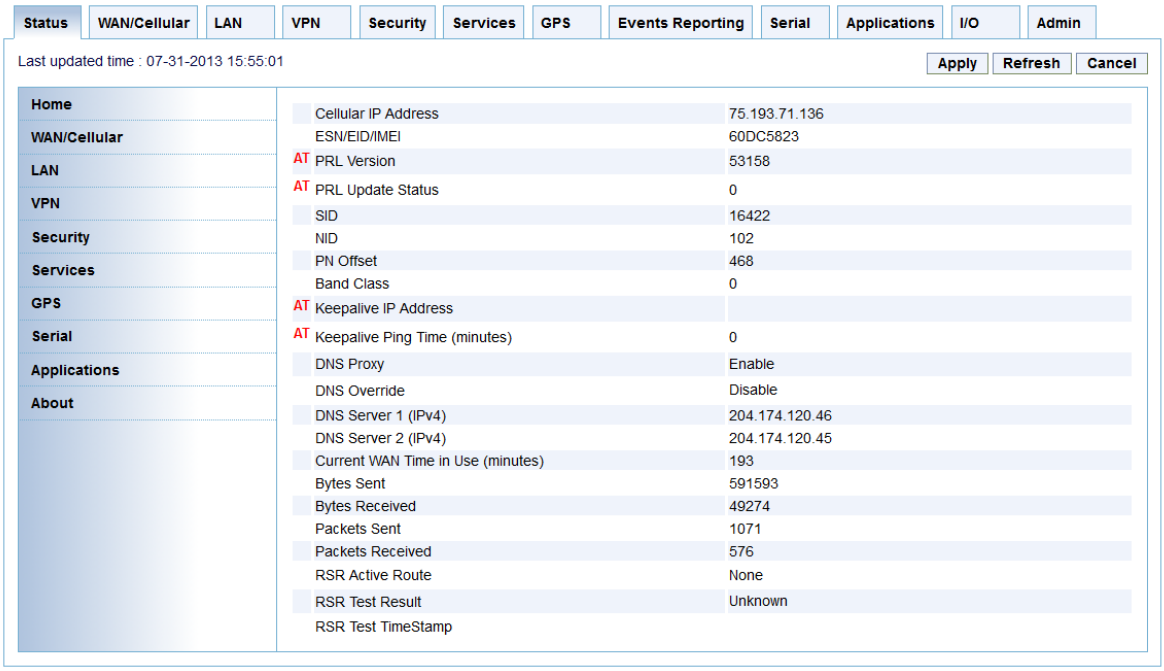


Figure 3-4: ACEmanager: Status > WAN/Cellular — CDMA

Field	Description
Cellular IP Address	Cellular IP Address assigned by the Mobile Network Operator.
ESN/EID/IMEI	Electronic Serial Number for the internal radio
PRL Version	Version of the Preferred Roaming List installed in the device
PRL Update Status	Status of the last PRL (Preferred Roaming List) update. 0 if there has been none
SID	System ID
NID	Network ID
PN Offset	Base station identifier used in CDMA networks
Band Class	CDMA band class
Keepalive IP Address	The IP address that WAN Keep Alive uses to test cellular connectivity (if enabled)
Keepalive Ping Time (minutes)	The amount of time between Keep Alive pings in minutes

Field	Description
DNS Proxy	Shows how the connected hosts acquire their DNS server. • Enable—DNS Proxy is activated. Connected hosts acquire the AirLink device's IP address as their DNS server. • Disable—DNS Proxy is deactivated. Connected hosts acquire the DNS server defined by the Mobile Network Operator as the first DNS server. To set this option, see DNS Proxy on page 94.
DNS Override	Override WAN-granted DNS
DNS Server 1 (IPv4)	1st DNS server IP address currently in use by the Network connection to resolve domain names into IP addresses
DNS Server 2 (IPv4)	2nd DNS server IP address
Current WAN Time in Use (minutes)	Provides the time (in minutes) that the WAN has been in use
Bytes Sent	Number of bytes sent to the cellular network since system startup or reboot
Bytes Received	Number of bytes received from the network since system startup or reboot
Packets Sent	Number of packets sent to the network since system startup or reboot
Packets Received	Number of packets received from the network since system startup or reboot
RSR Active Route	The active route status for Reliable Static Routing • Primary—Specified network traffic is currently using the configured primary route. • Backup—Specified network traffic is currently using the configured backup route. • None—RSR is not enabled.
RSR Test Result	Result of the most recent Tracking Object test
RSR Test TimeStamp	Time of the most recent Tracking Object test

GSM

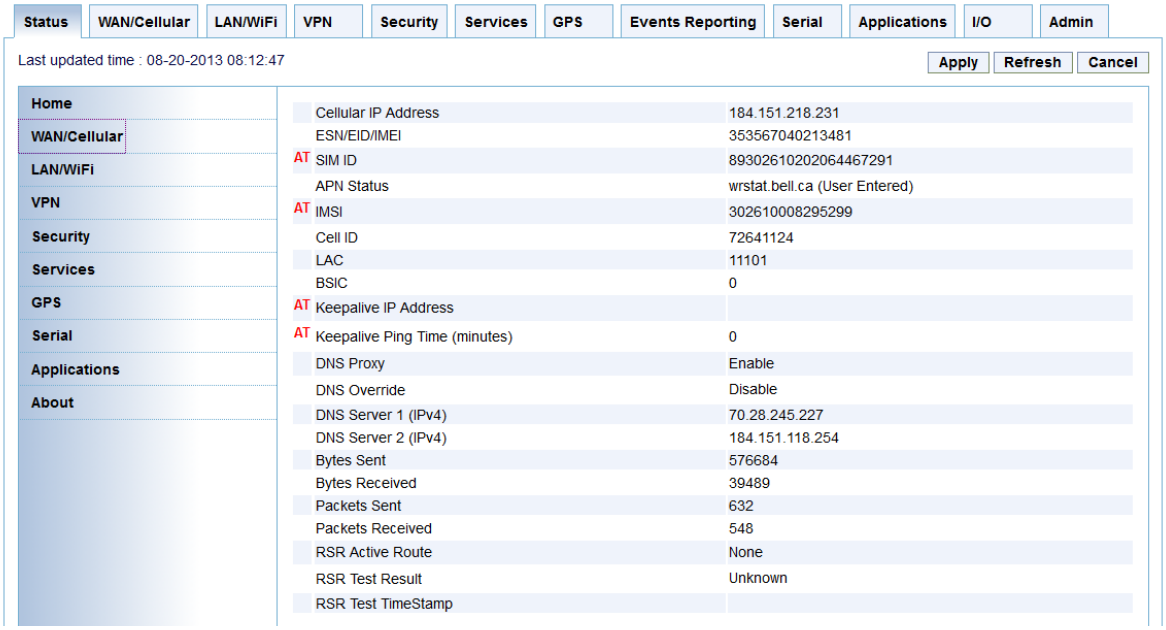


Figure 3-5: ACEmanager: Status > WAN/Cellular — GSM

Field	Description
Cellular IP Address	Cellular IP Address
ESN/EID/IMEI	Electronic Serial Number for the internal radio
SIM ID	Provides the identification number for the SIM card in use
APN Status	Identifies the current APN in use by the network connection • (Auto Configured) is a default APN based on the SIM card in use. • (User Entered) is a custom APN entered manually into the configuration. *Note: APN is configured on the WAN/Cellular configuration tab.*
IMSI	International Mobile Subscriber Identity number
Cell ID	A unique number that identifies each base transceiver station (BTS) or sector of a BTS within an LAC
LAC	Location Area Code
BSIC	Base Station Identity Code
Keepalive IP Address	The IP address that WAN Keep Alive uses to test cellular connectivity (if enabled)
Keepalive Ping Time (minutes)	The amount of time between Keep Alive pings in minutes

Field	Description
DNS Proxy	Shows how the connected hosts acquire their DNS server. • Enable—DNS Proxy is activated. Connected hosts acquire the AirLink device's IP address as their DNS server. • Disable—DNS Proxy is deactivated. Connected hosts acquire the DNS server defined by the Mobile Network Operator as the first DNS server. To set this option, see DNS Proxy on page 94.
DNS Override	Override WAN-granted DNS
DNS Server 1	1st DNS server IP address currently in use by the Network connection to resolve domain names into IP addresses
DNS Server 2	2nd DNS server IP address
Bytes Sent	Number of bytes sent to the cellular network since system startup or reboot
Bytes Received	Number of bytes received from the network since system startup or reboot
Packets Sent	Number of packets sent to the network since system startup or reboot
Packets Received	Number of packets received from the network since system startup or reboot
RSR Active Route	The active route for Reliable Static Routing • Primary—Specified network traffic is currently using the configured primary route. • Backup—Specified network traffic is currently using the configured backup route. • None—RSR is not enabled.
RSR Test Result	Result of the most recent Object Tracking test
RSR Test TimeStamp	Time of the most recent Object Tracking test

LTE—Fallback to EV-DO

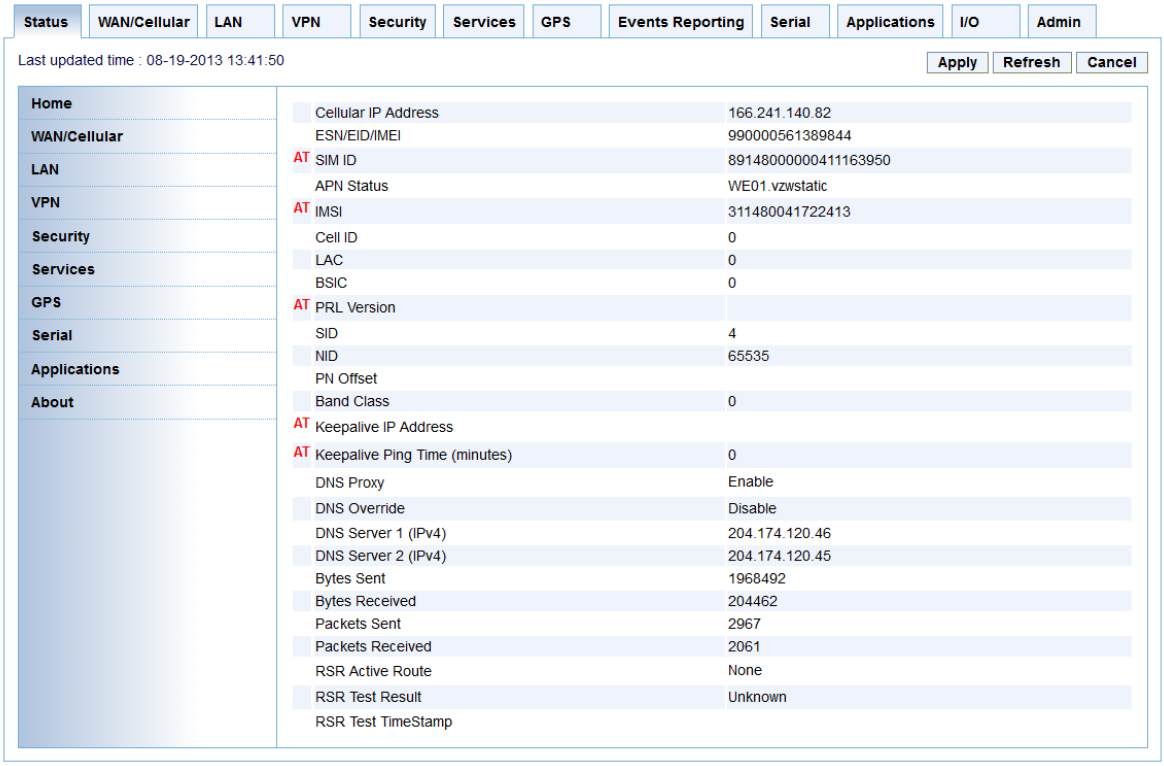


Figure 3-6: ACEmanager: Status > WAN/Cellular — LTE - Fallback to EV-DO

Field	Description
Cellular IP Address	Cellular IP Address
ESN/EID/IMEI	Electronic Serial Number for the internal radio
SIM ID	Provides the identification number for the SIM card in use
APN Status	Identifies the current APN in use by the network connection • (Auto Configured) is a default APN based on the SIM card in use. • (User Entered) is a custom APN entered manually into the configuration. *Note: APN is configured on the WAN/Cellular configuration tab.*
IMSI	International Mobile Subscriber Identity number
Cell ID	A unique number that identifies each base transceiver station (BTS) or sector of a BTS within an LAC
LAC	Location Area Code
BSIC	Base Station Identity Code

Field	Description
PRL Version	Version of the Preferred Roaming List installed in the device
SID	System ID
NID	Network ID
PN Offset	Base station identifier used in CDMA networks
Band Class	Radio frequency (For detailed information see LTE Networks on page 396.)
Keepalive IP Address	The IP address that WAN Keep Alive uses to test cellular connectivity (if enabled)
Keepalive Ping Time (minutes)	The amount of time between Keep Alive pings in minutes
DNS Proxy	Shows how the connected hosts acquire their DNS server. • Enable—DNS Proxy is activated. Connected hosts acquire the AirLink device's IP address as their DNS server. • Disable—DNS Proxy is deactivated. Connected hosts acquire the DNS server defined by the Mobile Network Operator as the first DNS server. To set this option, see DNS Proxy on page 94.
DNS Override	Override WAN-granted DNS
DNS Server 1	1st DNS server IP address currently in use by the Network connection to resolve domain names into IP addresses
DNS Server 2	2nd DNS server IP address
Bytes Sent	Number of bytes sent to the cellular network since the system startup or reboot
Bytes Received	Number of bytes received from the network since system startup or reboot
Packets Sent	Number of packets sent to the network since system startup or reboot
Packets Received	Number of packets received from the network since system startup or reboot
RSR Active Route	The active route for Reliable Static Routing • Primary—Specified network traffic is currently using the configured primary route. • Backup—Specified network traffic is currently using the configured backup route. • None—RSR is not enabled.
RSR Test Result	Result of the most recent Object Tracking test
RSR Test TimeStamp	Time of the most recent Object Tracking test

LTE—Fallback to GSM/HSPA+

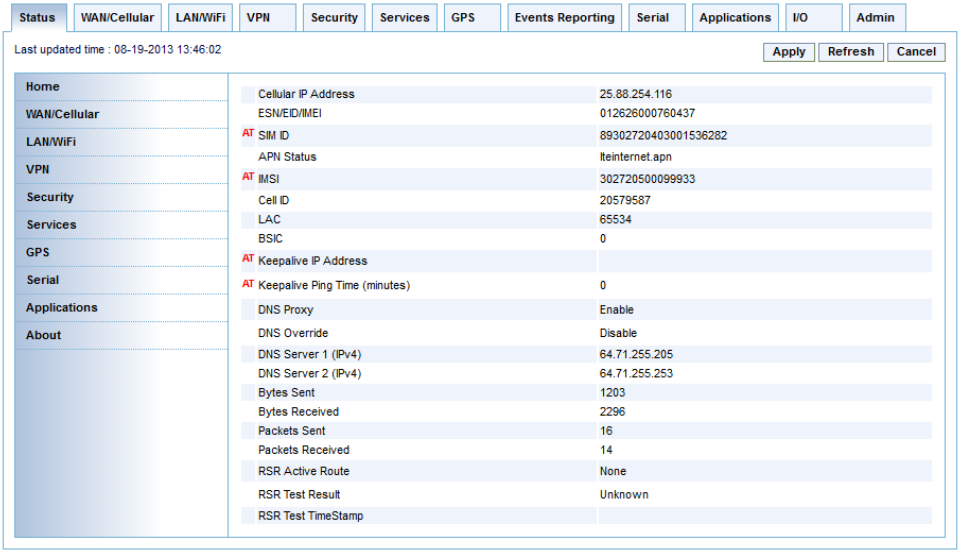


Figure 3-7: ACEmanager: Status > WAN/Cellular — LTE - Fallback to GSM/HSPA+

Field	Description
Cellular IP Address	Cellular IP Address
ESN/EID/IMEI	Electronic Serial Number for the internal radio
SIM ID	Provides the identification number for the SIM card in use
APN Status	Identifies the current APN in use by the network connection • (Auto Configured) is a default APN based on the SIM card in use. • (User Entered) is a custom APN entered manually into the configuration. *Note: APN is configured on the WAN/Cellular configuration tab.*
IMSI	International Mobile Subscriber Identity number
Cell ID	A unique number that identifies each base transceiver station (BTS) or sector of a BTS within an LAC
LAC	Location Area Code
BSIC	Base Station Identity Code
Keepalive IP Address	The IP address that WAN Keep Alive uses to test cellular connectivity (if enabled)
Keepalive Ping Time (minutes)	The amount of time between Keep Alive pings in minutes

Field	Description
DNS Proxy	Shows how the connected hosts acquire their DNS server. • Enable—DNS Proxy is activated. Connected hosts acquire the AirLink device's IP address as their DNS server. • Disable—DNS Proxy is deactivated. Connected hosts acquire the DNS server defined by the Mobile Network Operator as the first DNS server. To set this option, see DNS Proxy on page 94.
DNS Override	Override WAN-granted DNS
DNS Server 1	1st DNS server IP address currently in use by the Network connection to resolve domain names into IP addresses
DNS Server 2	2nd DNS server IP address
Bytes Sent	Number of bytes sent to the cellular network since the system startup or reboot
Bytes Received	Number of bytes received from the network since system startup or reboot
Packets Sent	Number of packets sent to the network since system startup or reboot
Packets Received	Number of packets received from the network since system startup or reboot
RSR Active Route	The active route for Reliable Static Routing • Primary—Specified network traffic is currently using the configured primary route. • Backup—Specified network traffic is currently using the configured backup route. • None—RSR is not enabled.
RSR Test Result	Result of the most recent Object Tracking test
RSR Test TimeStamp	Time of the most recent Object Tracking test

LAN

This is the status of the local network. It lists information about the network and connected clients.

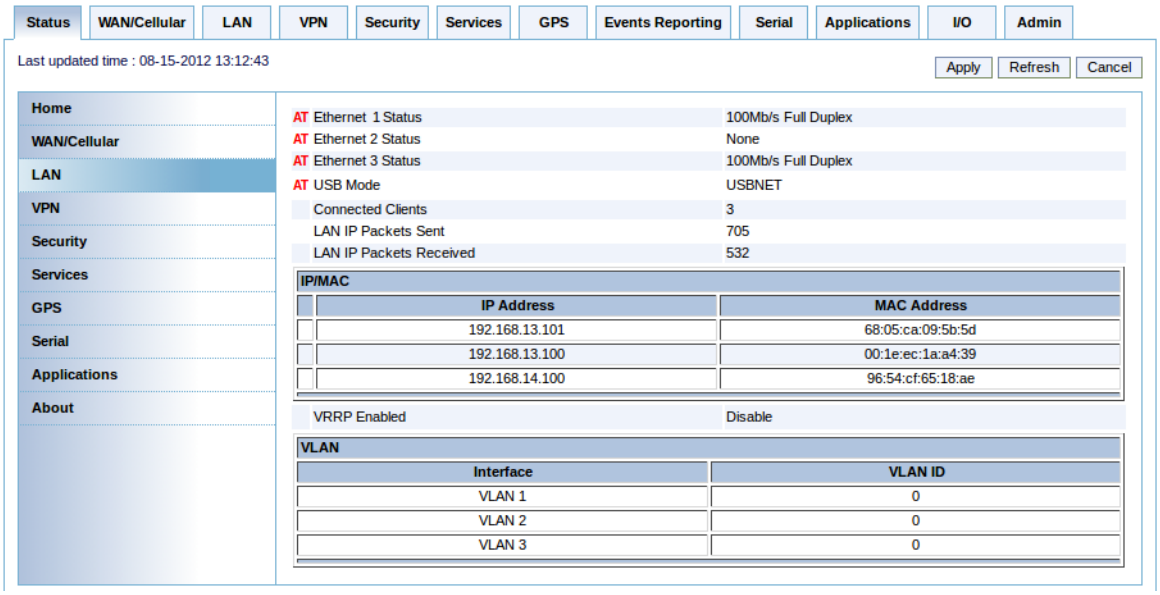


Figure 3-8: ACEmanager: Status > LAN (GX Series device with a Dual Ethernet X-Card installed)

Field	Description
Ethernet 1 Status	Speed and duplex status of the connection on Ethernet port 1 (the main Ethernet port). If there is no connection, the value is None.
Ethernet 2 Status	This field only appears on a GX Series device with a Dual Ethernet X-Card installed. Speed and duplex status of the connection on Ethernet port 2 on the Dual Ethernet X-Card. If there is no connection, the value is None.
Ethernet 3 Status	This field only appears on a GX Series device with a Dual Ethernet X-Card installed. Speed and duplex status of the connection on Ethernet port 3 on the Dual Ethernet X-Card. If there is no connection, the value is None.
USB Mode	Indicates which USB port mode is set: USBnet, USB serial, or Disabled.
Connected Clients	Number of connected hosts that obtained their IP address through DHCP over Ethernet or USBnet. The value in this field does not include hosts connected via PPP or PPPoE.
LAN IP Packets Sent	Number of IP packets sent to the Ethernet host interface since the system startup *Note: If the AirLink GX Series device has a Dual Ethernet X-Card installed, the data reported includes all three Ethernet ports.*

Field	Description
LAN IP Packets Received	Number of IP packets received from the Ethernet host interface since the system startup *Note: If the AirLink GX Series device has a Dual Ethernet X-Card installed, the data reported includes all three Ethernet ports.*
IP/MAC table	Displays the local IP Address and the MAC Address of connected hosts that obtain their IP address through DHCP.
VRRP Enabled	Indicates the configuration of the VRRP feature
VLAN table	Provides the identities (Interface name and ID) of the configured VLANs

LAN/WiFi

If you have a GX Series device with a Wi-Fi X-Card installed, there are some additional fields on the Status > LAN/WiFi screen, as shown in Figure 3-9.

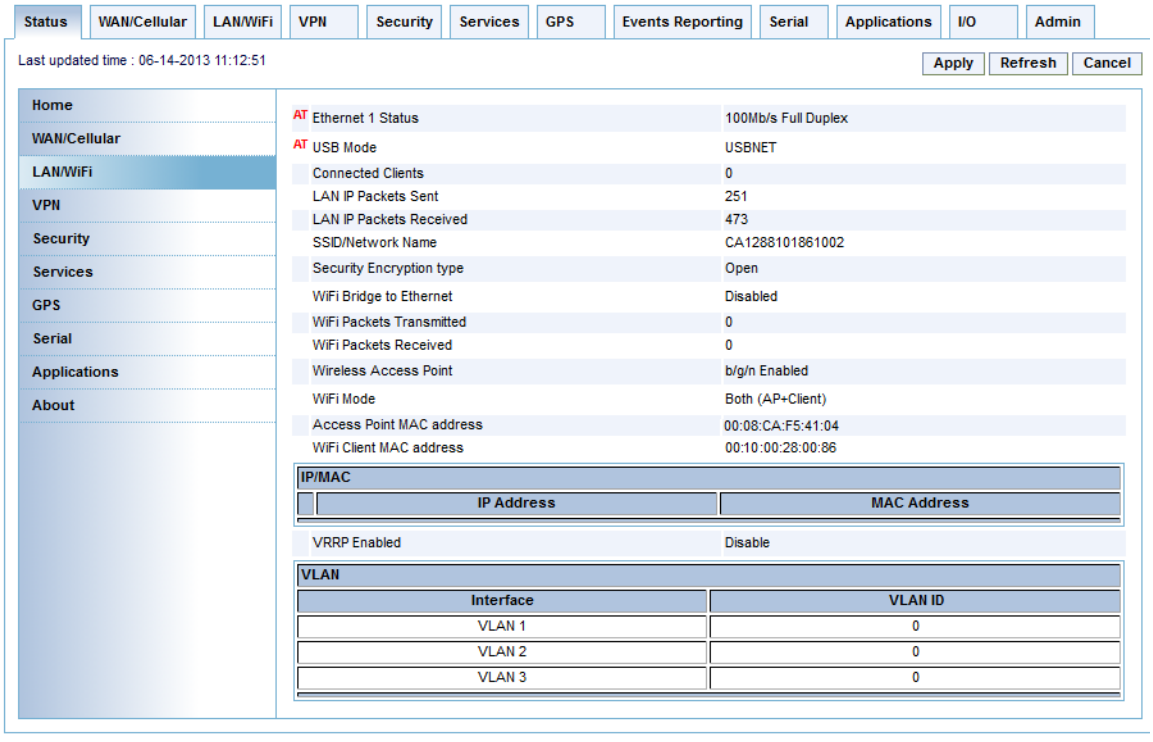


Figure 3-9: ACEmanager: Status > LAN/WiFi

Field	Description
Ethernet 1 Status	Speed and duplex status of the connection on Ethernet port 1 (the main Ethernet port). If there is no connection, the value is None.
USB Mode	See field descriptions starting on page 55.
Connected Clients	Number of connected hosts that obtained their IP address through DHCP over Ethernet, USBnet, and hosts connected via Wi-Fi. The value in this field does not include hosts connected via PPP or PPPoE.
LAN IP Packets Sent	See field descriptions starting on page 55.
LAN IP Packets Received	
SSID/Network Name	Shows the configured or default Wi-Fi SSID/Network name
Security Encryption type	Shows the Wi-Fi security encryption (security authentication) type
WiFi Bridge to Ethernet	Shows the status of the Bridge WiFi to Ethernet field. When this feature is enabled, the Ethernet LAN hosts and the Wi-Fi access point hosts are on the same subnet. For details, see Bridge WiFi to Ethernet on page 72.
WiFi Packets Transmitted	Number of IP packets sent to the access point host interface over Wi-Fi since the system startup
WiFi Packets Received	Number of IP packets received by the access point host interface over Wi-Fi since the system startup
Wireless Access Point	Indicates how the access point is configured. For more information, see Enable Wireless Access Point on page 87.
WiFi Mode	Wi-Fi mode. For more information, see Wi-Fi Mode on page 86.
Access Point MAC address	The MAC address hosts connect to when the GX Series device is configured as an access point. For more information, see Access Point Mode on page 86 and Both (AP + Client) Mode on page 92.
WiFi Client MAC address	The MAC address the GX Series device uses to connect to a Wi-Fi access point when it is configured for Client mode. For more information, see Client Mode on page 90 and Both (AP + Client) Mode on page 92.
IP/MAC table	See field descriptions starting on page 57.
VRRP Enabled	
VLAN table	

VPN

The VPN section gives an overview of the VPN settings and indicates whether a VPN connection has been made.

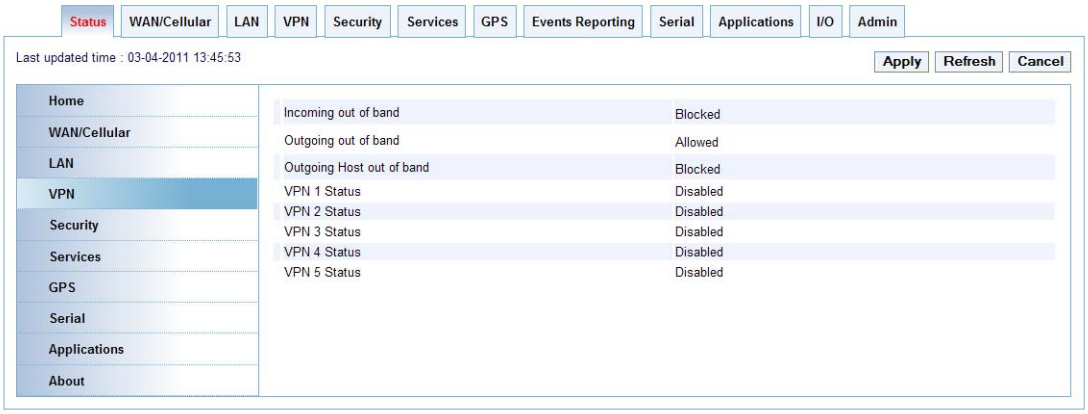


Figure 3-10: ACEmanager: Status > VPN

Field	Description
Incoming out of band	Indicates whether incoming out of band traffic is allowed or blocked
Outgoing out of band	Indicates whether outgoing ALEOS out of band traffic is allowed or blocked
Outgoing Host out of band	Indicates whether Outgoing Host out of band traffic is allowed or blocked
VPN 1 to 5 Status	The status of each IPsec VPN client or GRE client: Disabled, Enabled, or Connected. VPN 1, however, can be configured for L2TP and SSL VPN.

Security

The security section provides an overview of the security settings on the AirLink device.

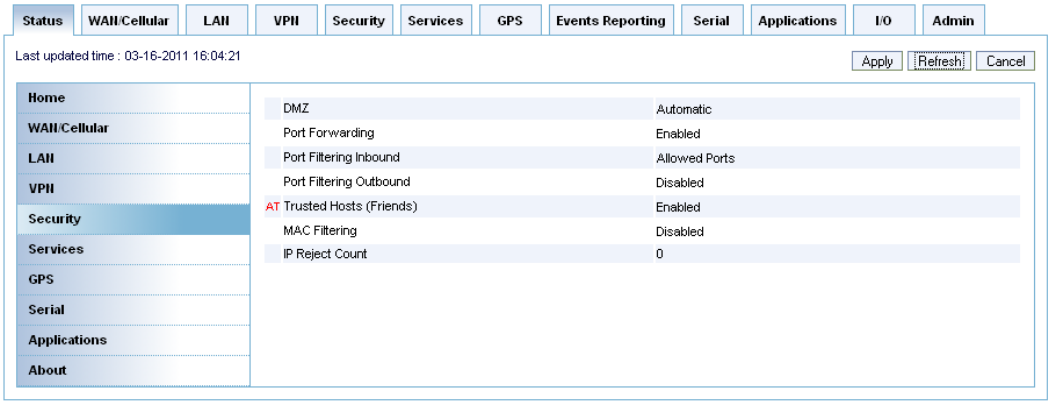


Figure 3-11: ACEmanager: Status > Security

Field	Description
DMZ	Options are: Automatic, Manual, or Disabled. DMZ defines a single LAN connected device where all unsolicited data should be routed.
Port Forwarding	Options are: Enabled or Disabled. Shows status of port forwarding
Port Filtering Inbound	Options are: Allowed Ports, Blocked Ports, or Not Used. Shows status of inbound port filtering
Port Filtering Outbound	Options are: Allowed Ports, Blocked Ports, or Not Used. Shows status of outbound port filtering
Trusted Hosts (Friends)	Options are: Disabled or Enabled. Accepts connections from only trusted remote IP addresses
MAC Filtering	Options are: Enabled or Disabled. Shows status of MAC filtering
IP Reject Count	Rejected IP Count

Services

This section shows the status of AirLink services, including the ACEmanager access level.

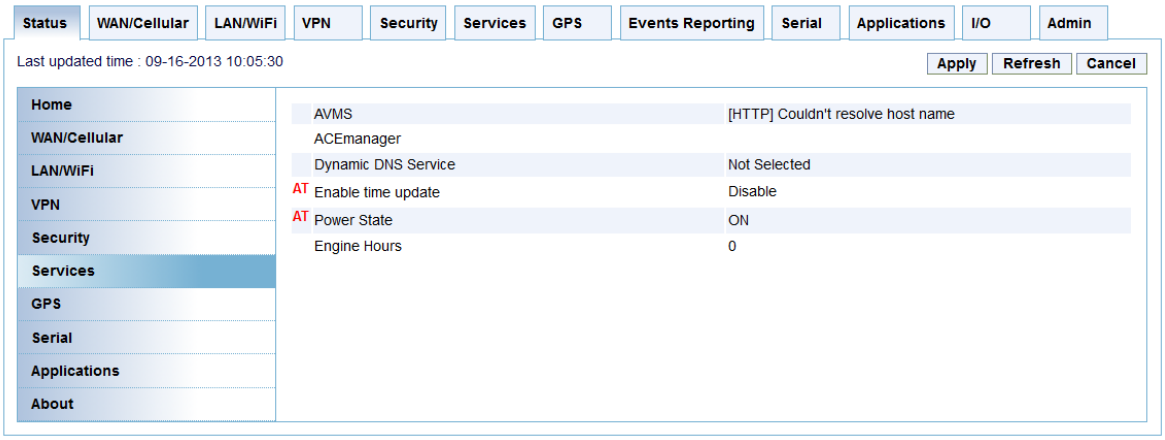


Figure 3-12: ACEmanager: Status > Services

Field	Description
AVMS	Indicates the status of the connection to the AirVantage Management Service. This field is blank if the AVMS configuration is disabled.
ACEmanager	The ACEmanager access mode. Options are Tethered Host and OTA or Tethered Host Only.
Dynamic DNS Service	Indicates the service in use for Dynamic DNS translation
Full Domain Name	If the Dynamic DNS Service is configured to use a 3rd party host, the domain name configured is displaced. If the Dynamic DNS Service is configured to use IP Manager, this field does not display.
Enable time update	Daily SNTP updates of the system time
Power State	The current state of the Low Power feature

GPS

The GPS (Global Positioning System) tab provides AirLink device location and movement information for use with tracking applications.

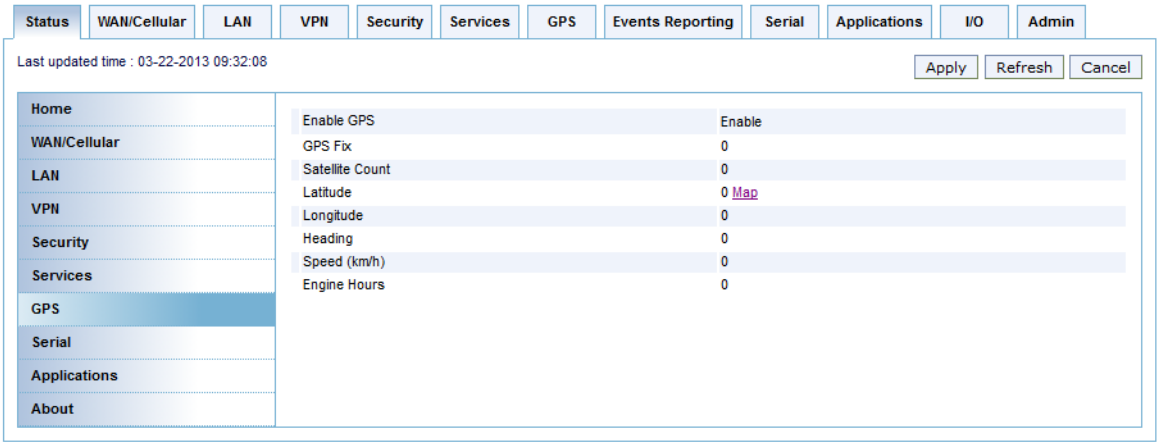


Figure 3-13: ACEmanager: Status > GPS

Field	Description
Enable GPS	Indicates that GPS is either enabled or disabled
GPS Fix	0 = No GPS Fix, 1 = GPS Fix Acquired, 2 = GPS WAAS Fix
Satellite Count	Shows how many satellites the GPS receiver detects
Latitude	Latitude of the GPS receiver
Longitude	Longitude of the GPS receiver
Heading	The direction in which the AirLink device is moving. No configuration is needed for Heading or Speed; they are calculated automatically.
Speed (km/h)	Speed (in kilometers per hour)
Engine Hours (Hours)	Measure of the number of hours the engine is on

Serial

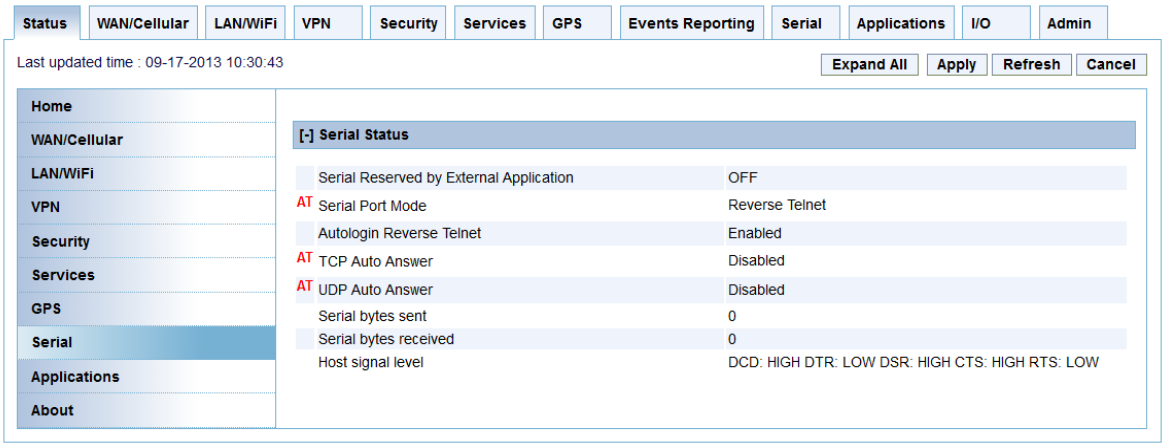


Figure 3-14: ACEmanager: Status > Serial

Field	Description
Serial Reserved by External Application	This field displays the reservation status of the serial port. • ON—The serial port is reserved for ALEOS Application Framework (ALEOS AF), and cannot be used for any other serial-related ALEOS features. • OFF— The serial port is available for non-ALEOS AF, serial-related ALEOS features. To reserve the serial port for ALEOS AF, go to Applications > ALEOS Application Framework > Serial Port Reserved. (See ALEOS Application Framework on page 250.)
Serial Port Mode	Default power-up mode for the serial port. When the AirLink device is power-cycled, the serial port enters the mode specified by this command after 5 seconds.
Autologin reverse telnet	This field only appears when reverse telnet is selected as the Serial Port Mode. Shows the status of autologin for reverse telnet. For more information, see Reverse Telnet/SSH on page 224.
TCP Auto Answer	This parameter determines how the AirLink device responds to an incoming TCP connection request. The AirLink device remains in AT Command mode until a connection request is received. DTR must be asserted (S211=1 or &D0) and the device must be set for a successful TCP connection. The AirLink device sends a “RING” string to the host. A “CONNECT” sent to the host indicates acknowledgment of the connection request and the TCP session is established. Options are: • Disabled (Default) • Enabled
UDP Auto Answer	Enables UDP auto answer (half-open) mode • Normal mode • Enable UDP auto answer mode
Serial bytes sent	Number of bytes sent over serial port to host
Serial bytes received	Number of bytes received over serial port from host

Field	Description
Serial Signal Level	Shows the status of the following parameters related to the host signal level: • DCD—Data Carrier Detect—Control signal to the PC • DTR—Data Terminal Ready—Used to establish a connection • DSR—Data Set Ready—Used to establish a connection • CTS—Clear to Send—Data flow control • RTS—Request to Send—Data flow control Each parameter can have a value of LOW (signal not asserted) or HIGH (signal being asserted). The first three parameters (DCD, DTR, and DSR) may be helpful for troubleshooting. If the values shown for these parameters are not as expected: **1.** Press Refresh to ensure you have the latest values. **2.** Check the cable connections. *Note: ACEmanager does not update dynamically. Press Refresh to view the current values.*
I/O X-Card Serial These fields apply only to GX Series devices with an I/O X-Card installed.	
I/O X-Card Serial Reserved by External Application	This field displays the reservation status of the I/O X-Card serial port. • ON—The serial port is reserved for ALEOS Application Framework (ALEOS AF), and cannot be used for any other serial-related ALEOS features. • OFF— The serial port is available for non-ALEOS AF, serial-related ALEOS features. To reserve the serial port for ALEOS AF, go to Applications > ALEOS Application Framework > Serial Port Reserved. (See ALEOS Application Framework on page 250.)
I/O X-Card Serial Port Mode	Default power-up mode for the I/O X-Card serial port. When the AirLink device is power-cycled, the serial port enters the mode specified by this command after 5 seconds.
I/O X-Card Serial TCP Auto Answer	This parameter determines how the AirLink device responds to an incoming TCP connection request on the I/O X-Card serial port. The AirLink device remains in AT Command mode until a connection request is received. DTR must be asserted (S211=1 or &D0) and the device must be set for a successful TCP connection. The AirLink device sends a “RING” string to the host. A “CONNECT” sent to the host indicates acknowledgment of the connection request and the TCP session is established. Options are: • Disabled (Default) • Enabled
I/O X-Card Serial UDP Auto Answer	Enables UDP auto answer (half-open) mode on the I/O X-Card serial port • Normal mode • Enable UDP auto answer mode
I/O X-Card Serial bytes sent	Number of bytes sent over the I/O X-Card serial port to host
I/O X-Card Serial bytes received	Number of bytes received over the I/O X-Card serial port from host

Applications

The Applications section of the Status group provides information on the status of the Garmin device and data service.

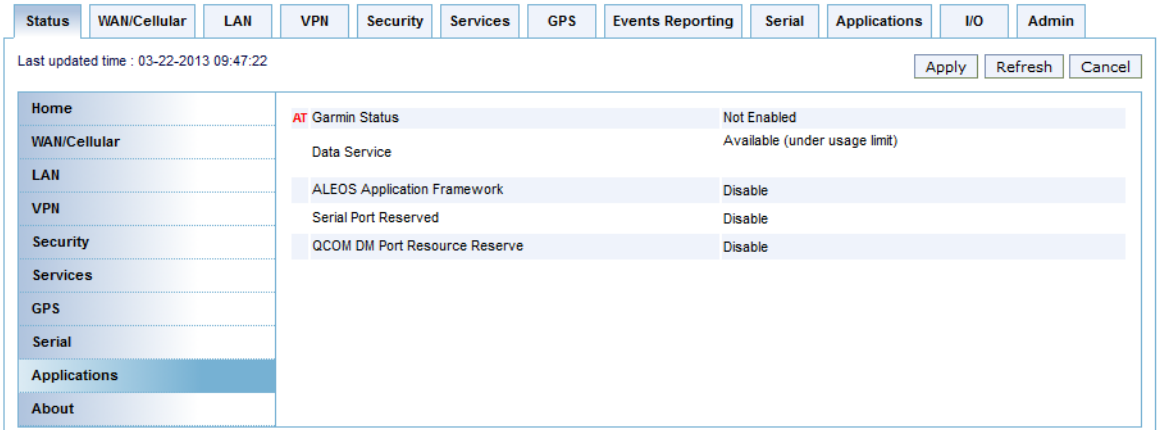


Figure 3-15: ACEmanager: Status > Applications

Field	Description
Garmin Status	The state of the connection to the Garmin device when it is enabled. This field is blank when the Garmin device is disabled.
Data Service	The Data Service field displays “Available (under usage limit)” if the configured usage limit has not been exceeded.
ALEOS Application Framework	Indicates whether ALEOS Application Framework is enabled or disabled
Serial Port Reserved	Disable (default) Enable
QCOM DM Port Resource Reserve	Disable (default) Enable

About

The About section of the Status group provides basic information about the cellular device. The fields for this section provide the same information for the CDMA, GSM, and LTE wireless standards.

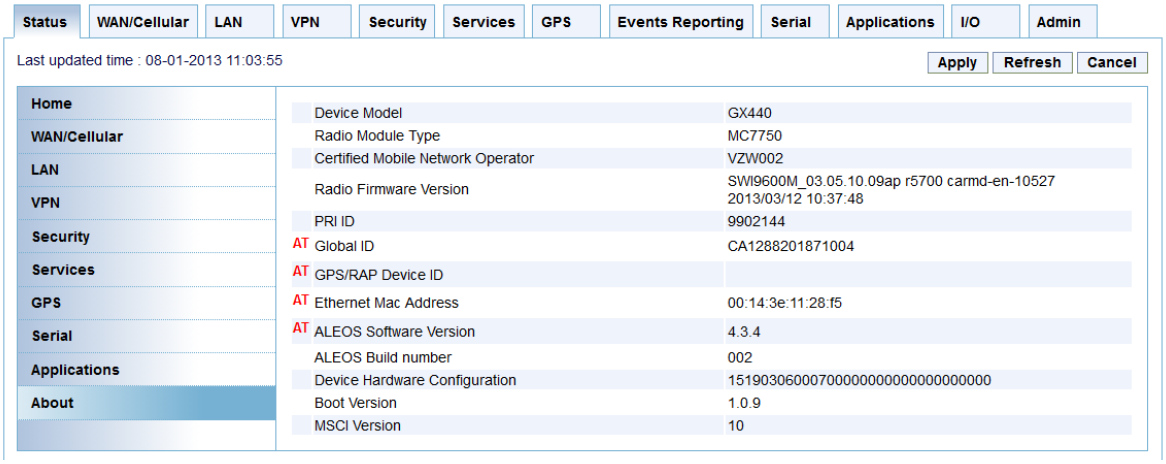


Figure 3-16: ACEmanager: Status > About

Field	Description
Device Model	Model of the device (e.g., GX400)
Radio Module Type	Model number of the internal cellular radio module (e.g. MC7700)
Certified Mobile Network Operator	Provides the name of the Mobile Network Operator whose network the AirLink device is connected to.
Radio Firmware Version	Firmware version in the radio module
PRI ID	Product Release Instructions ID number
Global ID	Device ID used by ALEOS to identify itself for various management applications
GPS/RAP Device ID	Device ID of GPS/RAP
Ethernet Mac Address	MAC address of the main Ethernet port
Ethernet 2 Mac Address	MAC address of Ethernet port 2 on the Dual Ethernet X-Card (Only appears if the device has a Dual Ethernet X-Card installed)
Ethernet 3 Mac Address	MAC address of Ethernet port 3 on the Dual Ethernet X-Card (Only appears if the device has a Dual Ethernet X-Card installed)
ALEOS Software Version	Displays the version of ALEOS software running on the AirLink Device
ALEOS Build number	The build number for the ALEOS Software
Device Hardware Configuration	Indicates the device's hardware configuration
Boot Version	Version of boot code installed in the device
MSCI Version	MSCI version of the ALEOS internal configuration database

4: LAN/Wi-Fi Configuration

4

Note: The LAN/WiFi tab in ACEmanager only appears when a Wi-Fi X-Card is installed in the AirLink GX Series device. If a Wi-Fi X-Card is not installed, this tab appears as LAN.

The primary purpose of the AirLink device is to route data between one or more connected devices and the Internet via the mobile network. The AirLink device has two modes you can use for configuring a LAN—Private Mode and Public Mode.

Private and Public Mode

Private Mode and Public Mode are Sierra Wireless terms.

In Private Mode, the AirLink device itself has a routable IP address from the MNO. Connected devices are assigned non-routable (private) IP addresses, making the connected router or laptop not directly accessible from the Internet.

In Public Mode the AirLink device passes the public routable IP address from the MNO through to the connected device such as a router or laptop, making the router or laptop publicly addressable for Internet applications. Figure 4-1 shows the two types of configurations.

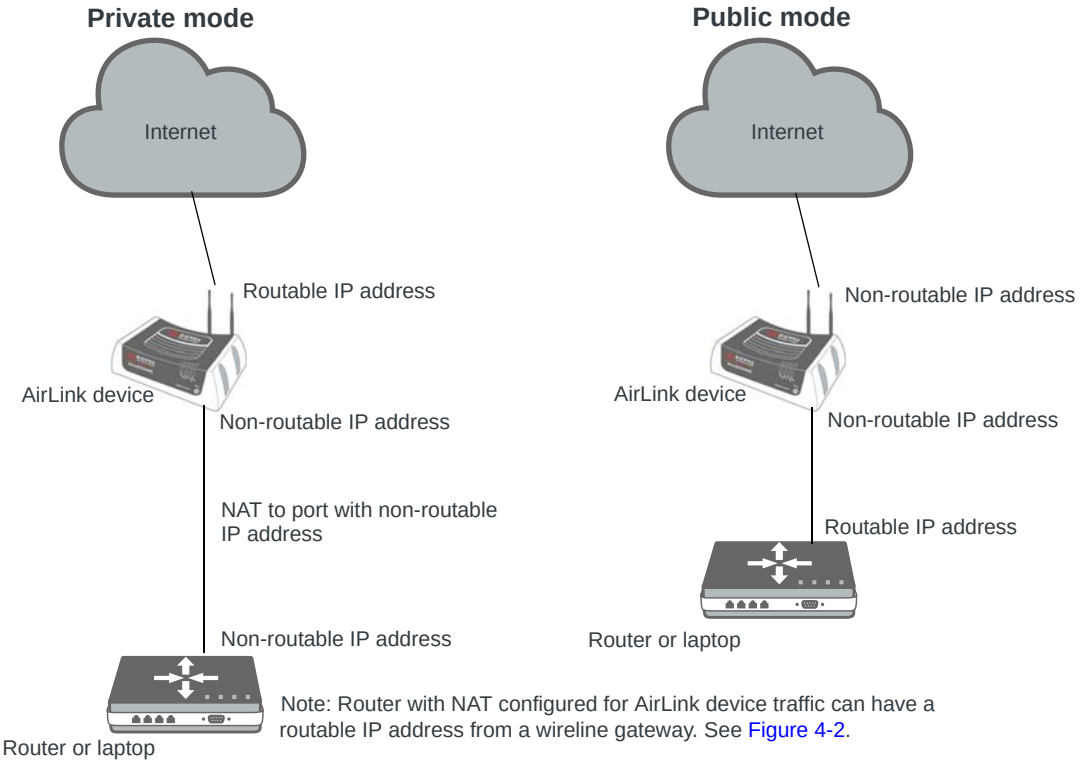


Figure 4-1: Private vs. Public Mode

Private Mode

Private Mode uses Network Address Translation (NAT) to enable the non-routable device to access the Internet. Data from the connected devices can be passed through the AirLink device and AirLink device applications such as SNMP have a routable IP address to target.

In a business continuity application where the router also has a routable IP address from a wireline gateway connection (as shown in Figure 4-2) the IT administrator may prefer to use that lower cost connection for AirLink device SNMP applications and use the reliable static route failover protocol to direct SNMP-like traffic out the wireline gateway connection, unless that connection has failed.

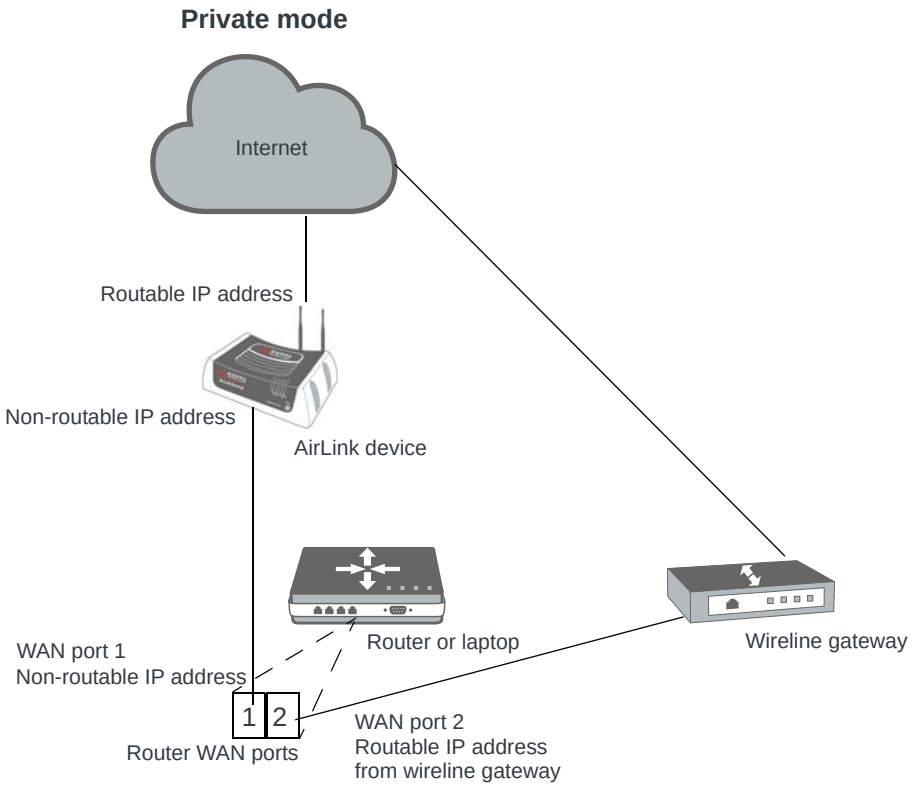


Figure 4-2: Private Mode for SNMP-like applications

Sierra Wireless recommends a Private Mode network as the most reliable configuration to use in a business continuity failover application as defined in the AirLink ES440 Hardware User Guide (or Figure 4-2) with Reliable Static Routing and Reverse Telnet. For more information, see Reliable Static Routing (RSR) on page 88 and Reverse Telnet/SSH on page 158.

Public Mode

Public Mode is similar to IP pass-through except that in Public Mode the IP address is also passed through from the MNO. The AirLink device acts like a pass-through data connection for all traffic from the MNO. Public Mode is required when the connected device needs a routable IP address and has no other connection to obtain it.

In Public Mode the AirLink device does not have a routable IP address and therefore applications such as SNMP on the AirLink device require hair-pinning from the routable IP address on the connected router back to the AirLink device, as shown in Figure 4-3, to serve SNMP-like applications. Sierra Wireless recommends this configuration for connecting PCs or other endpoints that are capable of responding to IP applications from the network. While hair-pinning on the router is an acceptable configuration, it means SNMP-like data from the AirLink device relies on the continuous operation of the router, whereas Private Mode uses NAT to avoid the hair-pinning requirement.

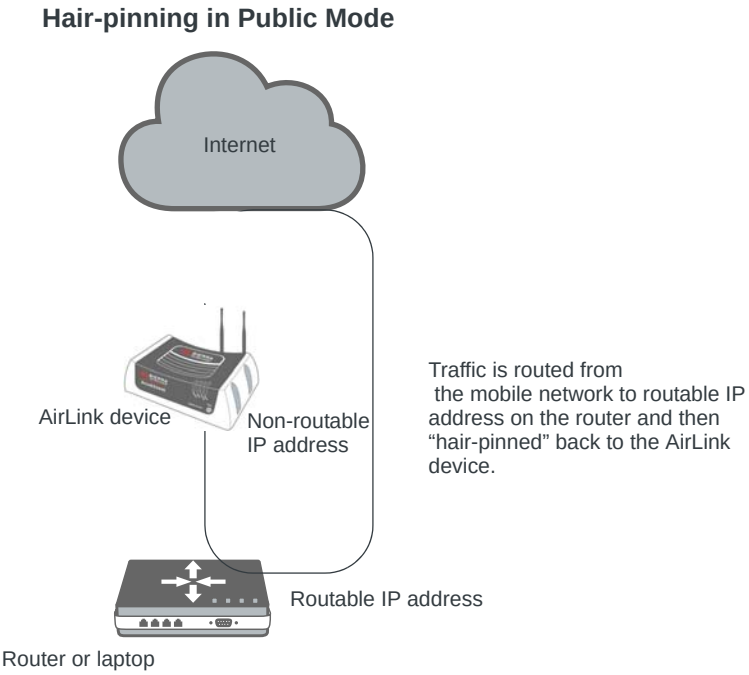


Figure 4-3: Hair-pinning in Public Mode

Tip: *When using Public mode, Sierra Wireless recommends connecting the device directly to the computer or other end device. Using a hub or switch may prevent the AirLink device from updating the IP address of the end device when an IP address is received from the cellular network.*

In ACEmanager, the Host Public mode and DHCP settings are part of the LAN tab**.** Subtabs of the LAN tab address the configuration of each interface or network type.

DHCP/Addressing

This section is primarily a status display of the configurations, with a few options that are global to all interface types. Interfaces that are enabled in the current configuration are displayed with their configured settings.

DHCP addresses and subnets are assigned to the LAN side interfaces display. If no Wi-Fi X-Card is installed in an AirLink GX Series device, select the DHCP/ Addressing section from the LAN tab to display a screen similar to the Figure 5-1 example.

Note: If the device has not been reset since configuration changes were made, the current configuration in use may be different.

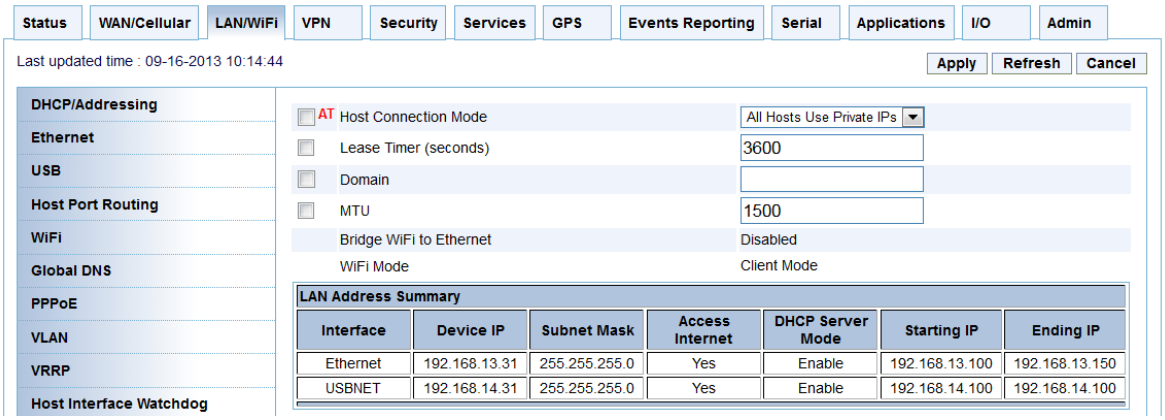


Figure 4-4: ACEmanager: LAN/Wi-Fi > DHCP/Addressing

If a Wi-Fi X-Card is installed in the AirLink GX Series device, the LAN tab changes to LAN/WiFi, and selecting DHCP/Addressing displays a screen similar to Figure 4-4. When Wi-Fi is bridged to Ethernet, the Bridge Wifi to Ethernet field displays Enabled, and Ethernet and Wi-Fi appear in the same subnet row.

Note: Bridging between WiFi and USB/net is not supported.

Field	Description
Host Connection Mode	Sets the Host Interface to use the Public IP address granted by the cellular network or private IP addresses. All host interfaces which are not using the public IP address use private IP addresses. The options are: • Ethernet Uses Public IP* • All Hosts Use Private IP—(Default) • USB Uses Public IP • RS232 Uses Public IP • First Host gets Public IP If you select this option, you do not have to specify the type of connection that uses the Public IP address. The first device to connect uses the Public IP address, regardless of whether it has a USB or Ethernet connection. For more information on Private and Public mode, see Private and Public Mode on page 67. **Caution:** ** If the AirLink GX Series device has a Dual Ethernet X-Card installed, selecting this option disables the additional Ethernet ports on the Dual Ethernet X-Card. The main Ethernet port is still functional.* *Note: The connected computer receives the DHCP address from ALEOS and it also provides a static route (192.168.13.31 by default) that allows you to access ACEmanager from a connected laptop.*
Public Mode Subnet Mask	Public Mode subnet mask indicates the range of Public Mode host IP addresses. Options are: • 255.255.255.0 (24-bit) Default • 255.255.255.255 (32-bit) Choose the option that matches the subnet mask received from the mobile network.
Lease Timer (seconds)	Configurable DHCP lease time The default lease for the GX Series and LS300 is 3600 seconds (1 hour). The lease timer applies to all Ethernet, USB/net, and Wi-Fi connected DHCP hosts.
Domain	Displays the DHCP domain name This domain name is passed to the DHCP host in option 15 of the DHCP packet.
MTU	Sets the maximum transmission unit size The maximum transmission unit size is sent to the DHCP host in option 26 of the DHCP packet. The default is 1500.
Bridge WiFi to Ethernet	Allows routing between the Ethernet Lan and Wi-Fi. When enabled, the Ethernet port and the Wi-Fi ports are on the same subnet. Options are: • Enabled (Default) • Disabled This field is only available when a Wi-Fi X-card is installed.
WiFi Mode	Indicates the Wi-Fi module mode This field is only available when a Wi-Fi X-card is installed.
WAN IP Address	Displays the WAN IP address when the Wi-Fi is used in client mode for WAN connectivity

Field	Description
LAN Address Summary	Displays the interfaces which have been enabled. By default, only the Ethernet and USBNET Interfaces are enabled.
Interface	The physical interface port or VLAN ID
Device IP	The IP address of the AirLink device for the specified interface port. By default, this is set to 192.168.13.31 for Ethernet/WiFi and 192.168.14.31 for USB/net.
Subnet Mask	Subnet mask indicates the range of host IP addresses that can be reached directly. Changing this limits or expands the number of clients that can connect to the AirLink device. The default of 255.255.255.0 means that 254 clients can connect to the AirLink device. Uses 192.168.13. as the first three octets of the IP address if the device IP is 192.168.13.31.
Access Internet	Appears if the interface is configured to allow connected host(s) access to the Internet *Note: Internet access cannot be disabled for Ethernet or Wi-Fi hosts.*
DHCP Server Mode	Indicates whether or not the interface has a DHCP server enabled to provide dynamically allocated IP addresses provided to connected hosts
Starting IP	Ethernet DHCP pool starting IP address
Ending IP	The ending IP for the interface. If the starting and ending IP are the same, there is a single address in the pool and only one host receives an IP address from the DHCP server for that interface. Some interfaces, such as USB, can only have a single host connection. For others, statically assigned IP addresses in the same subnet, but outside of the DHCP pool, can still connect and use the device in the same way as a DHCP connected host.

Tip: *If you are using Private Mode for all hosts (*HOSTPRIVMODE=1), make sure that device IP, Starting IP, and Ending IP are on the same subnet defined by the DHCP network mask. If the subnet mask is 255.255.255.0, it is safe to use 192.168.x.y for each as long as the x is the same number (0 in the example screen shot above) and the y is different (1 and 2 in the example) and between 0 and 254.*

Internal DHCP Server

DHCP (Dynamic Host Configuration Protocol) has become a primary component of today's network environments. DHCP allows one server to automatically and dynamically allocate network IP addresses and other network related settings (such as subnet masks, routers, etc.) to each computer or device without the need to set up each specifically or keep track of what addresses have already been used.

In a default configuration, the AirLink device acts as a DHCP host to any device connected to its ports. This DHCP host provides that device with an IP address that can be used to communicate on the Internet.

Address Assignment in Public Mode

1. When the AirLink device registers on the cellular network, it is assigned an IP address from the carrier, e.g., 10.1.2.0.

2. When using a specific interface, the AirLink device acts as a DHCP server unless disabled. When the Host Connection Mode is Ethernet Uses Public IP, and the AirLink device receives a DHCP request from an Ethernet device connected to its ports, it hands off the assigned address to the device and sets up the default gateway address as 10.1.2.1. If the fourth octet value is already a 1, it assigns 10.1.2.2 as the router address.

Note: The primary gateway to the cellular network, for any connected device, is enabled by default.

3. The AirLink device also sends a /24 netmask (255.255.255.0 by default) and sets up a static route which maps 192.168.13.31 (or the address configured with *HOSTPEERIP if it is changed) to 10.1.2.1 (or 10.1.2.2 if that was what the gateway address was given as).

Tip: *When PPPoE is used with the AirLink device, the DHCP server needs to be disabled. A tunnel is set up connecting a device (such as your computer or a router) with the AirLink device. The device then uses the MAC address of the AirLink device to send all outgoing packets.*

Ethernet

The AirLink device is equipped with an Ethernet port that can be enabled or disabled as needed. When the port is disabled, the host cannot connect via Ethernet, and ARP queries do not receive responses on the port.

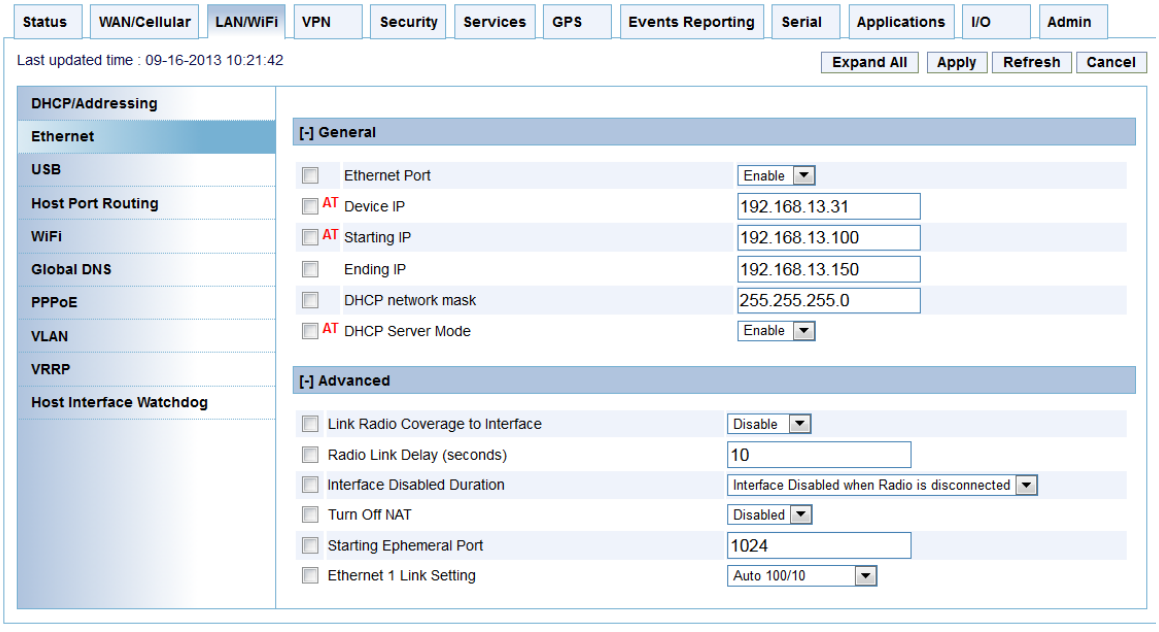
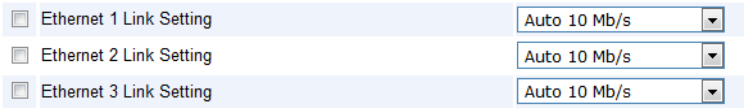


Figure 4-5: ACEmanager: LAN > Ethernet

Field	Description
General	
Ethernet Port	Enabled or Disabled *Note: When the port is disabled, the device ignores any physical connection to the Ethernet port.*
Device IP	The Ethernet IP address of the AirLink device. By default this is set to 192.168.13.31.
Starting IP	Ethernet DHCP pool starting IP address *Note: If only one computer or device is connected directly to the Ethernet port, this is the IP address it is assigned.*
Ending IP	The ending IP address for the Ethernet interface DHCP pool
DHCP network mask	The Netmask given to any Ethernet DHCP client
DHCP Server Mode	Enabled or disabled. By default, the Ethernet DHCP server is enabled. Disabling the DHCP server requires all connected clients to have static IP addressing. Static IP hosts need to be within the same subnet as defined by the device IP and DHCP network mask.
Advanced	
Link Radio coverage to Interface	This disables the specified port when there is no cellular coverage. Options are: • Disable (default) • Ethernet • USB
Radio Link Delay (seconds)	The delay in seconds before the selected interface goes down when there is no cellular coverage
Interface Disabled Duration	Sets the period of time (in seconds) that the LAN interface is disabled when linking a LAN port to radio coverage. Either the Ethernet or the USB LAN port can be linked to the radio coverage, but not at the same time. Options are: • Interface Disabled when Radio is disconnected (Default) • 5 Sec • 10 Sec • 15 Sec • 20 Sec • 25 Sec • 30 Sec
Turn Off NAT	When enabled, ALEOS routes packets without performing NAT on them. Options: Disabled (default) and Enabled.

Field	Description
Starting Ephemeral Port	This field allows you to set the starting port range used by a LAN host as the source port for over-the-air (OTA) destinations using NAT. *Note: This field is intended for advanced users only. In most cases, use the default value.* The NAT for the LAN host uses a range of 1000 ports as source ports for OTA destinations beginning with the configured Ephemeral port. Options are: • 1024 (default)–64535 If you have a network with multiple LAN hosts that are sending data to the same server and the server is not receiving data from one (or more) of the hosts, it may be because the Mobile Network Operator has a WAN firewall that is blocking the ports used by the NAT for over-the-air (OTA) destinations. This field enables you to avoid the blocked ports by changing the source port range used to send the data. For example, some users have found that changing the starting port to 42000 has resolved the issue. *Note: The ephemeral port setting does not affect any outbound traffic initiated by the device such as GPS reports, serial PAD or Modbus, Events Reporting, Device Initiated AVMS connection, etc.*
Ethernet 1 Link Setting **Ethernet 2 Link Setting** **Ethernet 3 Link Setting**	Configures the Ethernet port speed and duplex setting Most of the time you can leave the default setting and the device you are connecting automatically negotiates the speed and duplex setting with the AirLink device. However, if the connected device has a fixed setting, use this field to change the AirLink device setting to match that of the connected device. The options are: • Auto 100/10 (default) • Auto 10 Mb only • 100 Mb Full Duplex • 100 Mb Half Duplex • 10 Mb Full Duplex • 10 Mb Half Duplex If you have a GX Series device with a Dual Ethernet X-Card installed, ACEmanager displays separate fields for each Ethernet port.  You can view the current speed and duplex setting on the Status > LAN window. See page 55.

USB

The AirLink device is equipped with a USB port that increases the methods by which you can send and receive data from a connected computer. You can set up the USB port to work as either a virtual Ethernet port or a virtual serial port, or you can disable it to prevent access by USB. A driver installation is required to use the USB port in either mode.

By default, the port is set to work as a virtual Ethernet port.

Note: Sierra Wireless recommends that you use a USB 2.0 cable with your AirLink device and connect directly to your computer for best throughput.

To change the USB port to allow virtual serial port communication:

1. In ACEmanager, go to LAN > USB, and choose USB Serial as the USB Device Mode.

   To disable the USB port, select Disable from the same menu.

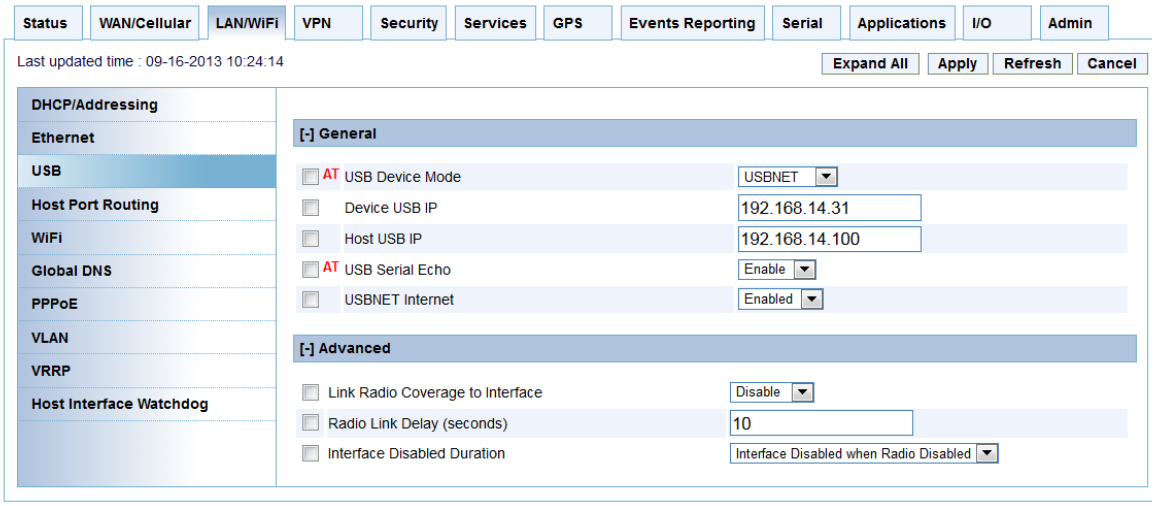


Figure 4-6: ACEmanager: LAN > USB

Note: There are USB/net and USB/serial drivers available for Windows XP and Windows 7 32-bit with a separate pair of drivers for Windows 7 64-bit. USB/serial also works with Linux CDC-ACM drivers.

Note: A reboot is required to activate the USB mode change.

Field	Description
General	
USB Device Mode	*USBDEVICE=n • 0 — USB Serial • 1 — USBNET • 2 — Disabled This parameter alters the default startup data mode for the USB port. *Note: If you want to stream GPS data to the USB port (Local/Streaming on page 198), set this field to USB Serial.*

Field	Description
Device USB IP	The USB/net IP address of the AirLink device. By default this is set to 192.168.14.31.
Host USB IP	The IP for the computer or device connected to the USB port
USB Serial Echo	Toggles AT command echo mode when the USB is configured for virtual serial 0 = OFF; 1 = ON
USBNET Internet	Enabled (default) or Disabled
Advanced	
Link Radio Coverage to Interface	Disables the specified port when there is no cellular coverage. Options are: • Disable (default) • Ethernet • USB
Radio Link Delay (secs)	The delay in seconds before the selected interface goes down when there is no cellular coverage
Interface Disabled Duration	Sets the period of time (in seconds) that the LAN interface is disabled when linking a LAN port to radio coverage. Either the Ethernet or the USB LAN port can be linked to the radio coverage, but not at the same time. Options are: • Interface Disabled when Radio is disconnected (Default) • 5 Sec • 10 Sec • 15 Sec • 20 Sec • 25 Sec • 30 Sec

Installing the USB Drivers for Windows

Virtual Ethernet is the default setting for the USB port. If you want to install the virtual serial port, change the Device Mode to USB Serial.

When you connect the AirLink device to a USB port on your computer for the first time, Windows detects a new device and prompts you to install the driver.

Note: The directions in this section are for Windows XP. To install the drivers under Windows 7, start the driver installation from the Windows Device Manager.

Note: Windows sees each port type as a different USB device and sees every port on your computer separately. If you change the port type on the AirLink device or connect to a different USB port on your computer or hub, Windows sees it as a new device.

Found New Hardware Wizard
Welcome to the Found New Hardware Wizard
Windows will search for current and updated software by looking on your computer, on the hardware installation CD, or on the Windows Update Web site (with your permission).
Read our privacy policy
Can Windows connect to Windows Update to search for software?
Yes, this time only
Yes, now and every time I connect a device
No, not this time
Click Next to continue.
< Back
Next >
Cancel

Figure 4-7: Found New Hardware Wizard

1. To start the install of the USB virtual Ethernet driver, select No, not this time and click Next.
2. Select Install from a list of specific location and click Next.

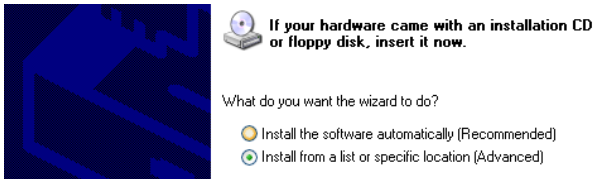

If your hardware came with an installation CD or floppy disk, insert it now.
What do you want the wizard to do?
Install the software automatically (Recommended)
Install from a list or specific location (Advanced)

Figure 4-8: Hardware Wizard: Location options

3. Select and/or enter the location of the driver.
   - If the driver is on the CD and the CD is in your drive, you can just select Search removable media.
   - If you have installed ACEmanager or the Setup Wizard, the drivers have been conveniently copied to your hard drive. Enter C:\Program Files\Common Files\AirLink as the location to search.
   - If you are installing the driver from a file downloaded from the Sierra Wireless website, select Include this location in the search and type in the location where you downloaded the file.
4. Click Next.

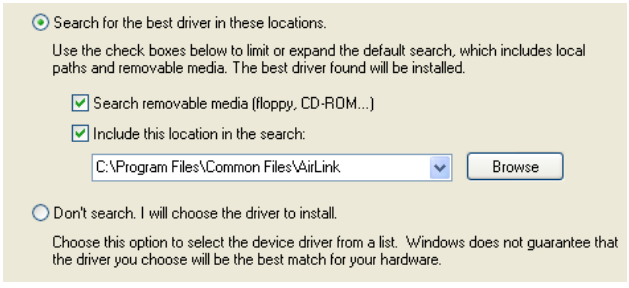

Search for the best driver in these locations.
Use the check boxes below to limit or expand the default search, which includes local paths and removable media. The best driver found will be installed.
Search removable media (floppy, CD-ROM...)
Include this location in the search:
C:\Program Files\Common Files\AirLink
Browse
Don't search. I will choose the driver to install.
Choose this option to select the device driver from a list. Windows does not guarantee that the driver you choose will be the best match for your hardware.

Figure 4-9: Hardware Wizard: Install location

After you select the location, the installation should begin. If you get a message asking if you want to continue the installation, click Continue Anyway.

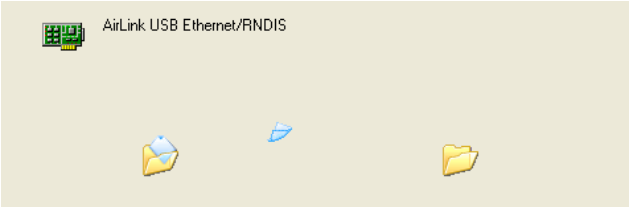


Figure 4-10: Hardware Wizard: Installing

5. Click Finish to complete the installation. The driver should be enabled without any need to reboot your computer.

Completing the Found New Hardware Wizard
The wizard has finished installing the software for:
AirLink USB Ethernet/RNDIS

Figure 4-11: Hardware Wizard: Finish

Virtual Ethernet

The USB Ethernet connection appears in your Network Connections window as a Local Area Connection.

Tip: *If you also have an Ethernet card on the computer, or have installed the USB Ethernet to more than one USB port on your computer, the USB Ethernet may show up with a number.*

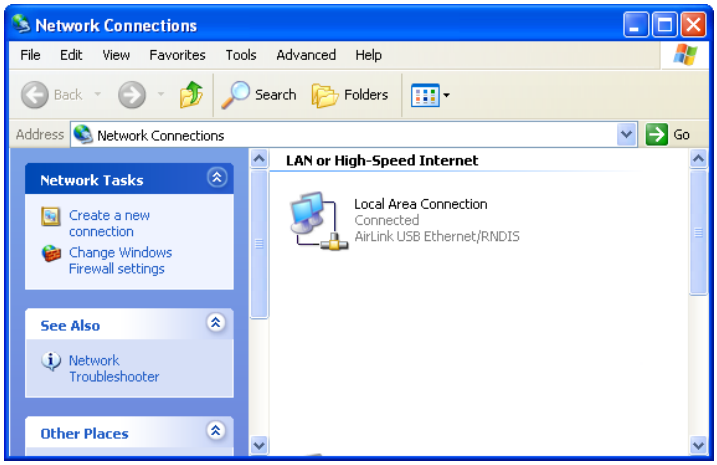


Figure 4-12: Network Connections

Note: By default, your Host IP for USB/net is 192.168.14.100.

You can also verify the installation by looking in the Device Manager.

1. Click Start > Control Panel.
2. Double-click the System icon.

3. Select the Hardware tab, and click the Device Manager button.

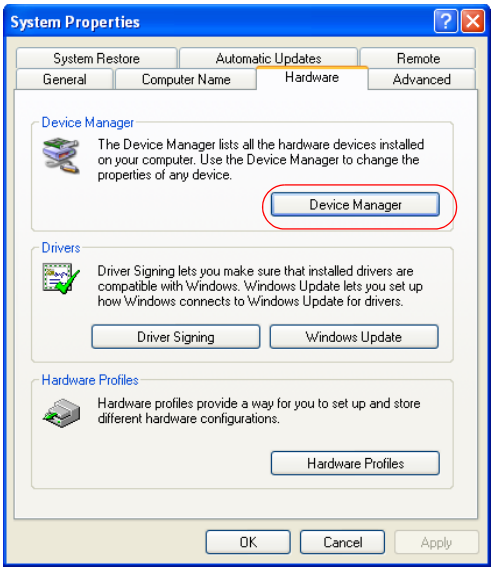

System Properties
System Restore
Automatic Updates
Remote
General
Computer Name
Hardware
Advanced
Device Manager
The Device Manager lists all the hardware devices installed on your computer. Use the Device Manager to change the properties of any device.
Device Manager
Drivers
Driver Signing lets you make sure that installed drivers are compatible with Windows. Windows Update lets you set up how Windows connects to Windows Update for drivers.
Driver Signing
Windows Update
Hardware Profiles
Hardware profiles provide a way for you to set up and store different hardware configurations.
Hardware Profiles
OK
Cancel
Apply

Figure 4-13: System Properties

4. Click the + in front of *Network Adapters*.

The newly installed driver, AirLink USB Ethernet/RNDIS, should appear. If the driver is shown with a # and number behind the driver name (e.g., AirLink USB Ethernet/RNDIS #2), more than one is installed on your computer, most likely for a different USB port. More than one copy of the driver should not cause any problems since only the connected port and its driver would be active.

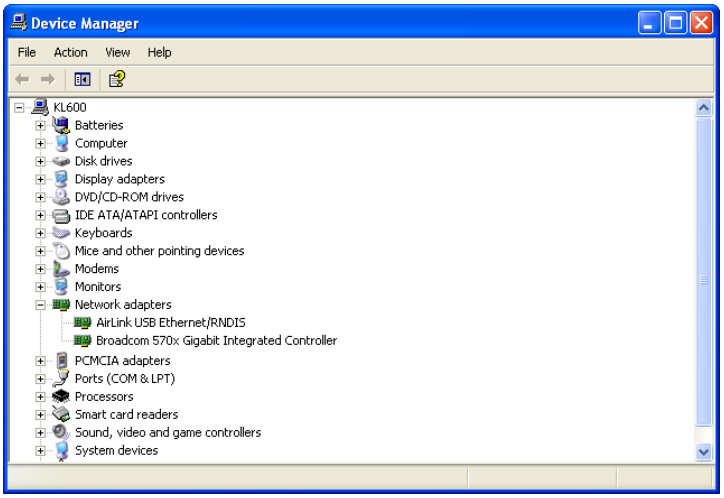


Figure 4-14: Device Manager > Ethernet

Once the driver is installed, you can use the USB port just like a standard Ethernet port.

Virtual Serial

Verify the installation by looking in the Device Manager.

1. Click Start > Control Panel.
2. Double-click the System icon.
3. Select the Hardware tab, and click the Device Manager button.

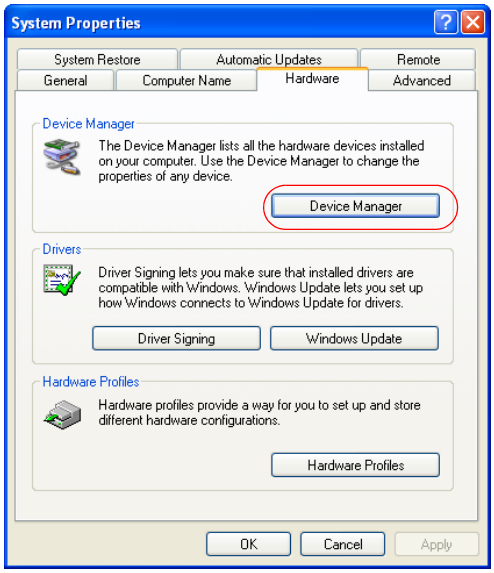

System Properties
System Restore
Automatic Updates
Remote
General
Computer Name
Hardware
Advanced
Device Manager
The Device Manager lists all the hardware devices installed on your computer. Use the Device Manager to change the properties of any device.
Device Manager
Drivers
Driver Signing lets you make sure that installed drivers are compatible with Windows. Windows Update lets you set up how Windows connects to Windows Update for drivers.
Driver Signing
Windows Update
Hardware Profiles
Hardware profiles provide a way for you to set up and store different hardware configurations.
Hardware Profiles
OK
Cancel
Apply

Figure 4-15: System Properties

4. Click the + in front of *devices*.

The newly installed driver, AirLink USB Serial Port, should appear.

Tip: *If the driver is shown with a number sign (#) and number behind the driver name (e.g., AirLink USB Serial Port #2), more than one driver is installed on your computer, most likely for a different USB port. More than one copy of the driver should not cause any problems since only the connected port and its driver would be active.*

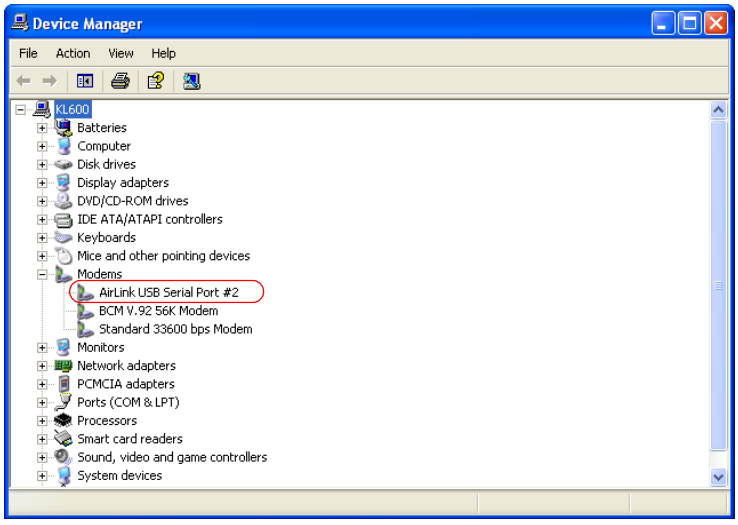


Figure 4-16: Device Manager > Serial

To connect to the device using the USB virtual serial, most applications or utilities require you to select or enter the serial (COM) port number. The USB connection appears as a standard serial port, so you need to determine its number to connect to it. The driver installation automatically assigns a port, or you can change it if you wish to another unused port.

5. From the Device Manager, right-click the driver name and select Properties.

Figure 4-17: Device Manager: Driver menu

6. Select the Advanced tab and click the Advanced Port Settings button.

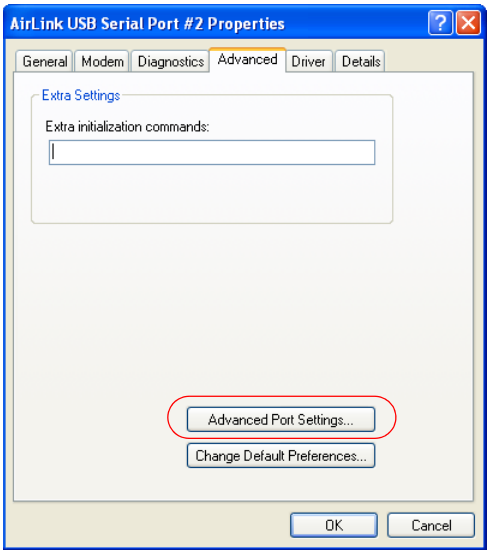


Figure 4-18: Driver Properties

7. The current port used is shown at the bottom of the screen. Use the drop-down menu to select an available COM port number if you need to change it.

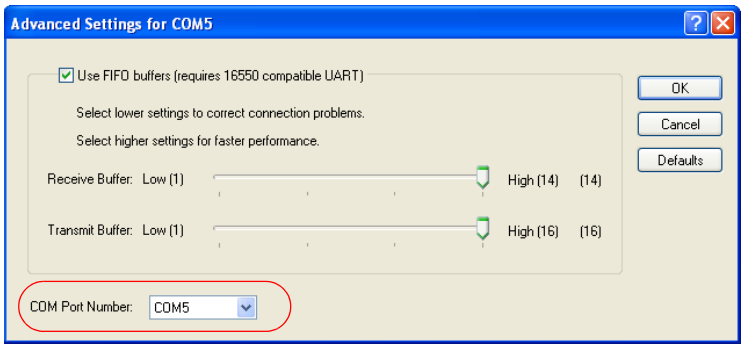

Advanced Settings for COM5
Use FIFO buffers (requires 16550 compatible UART)
Select lower settings to correct connection problems.
Select higher settings for faster performance.
Receive Buffer: Low (1) High (14) (14)
Transmit Buffer: Low (1) High (16) (16)
COM Port Number: COM5
OK
Cancel
Defaults

Figure 4-19: Advanced Settings

Note: The COM port number assigned by driver installation is the next port that is available.The port number might vary depending on the number of devices connected (using serial or virtual serial).

Once the driver is installed, you can use the USB port just like a standard serial port.

Host Port Routing

The Host Network is the equivalent of the IP route command.

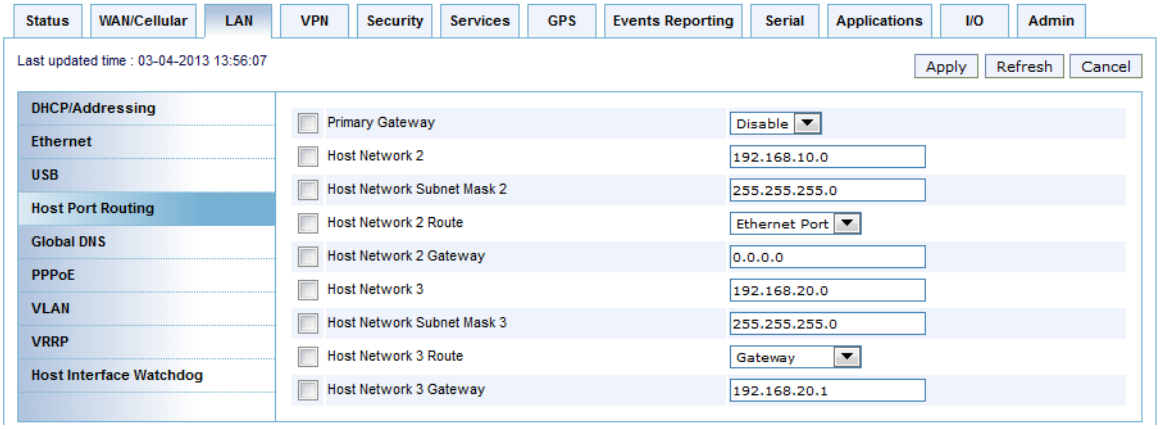


Figure 4-20: ACEmanager: LAN > Host Port Routing

Field	Description
Primary Gateway	When enabled, your device is the Primary Gateway for the network behind a router connected to it. ALEOS responds to ARPs for all non-host Ethernet subnets.
Host Network 2 and Host Network 3	Network to route to host interface connected to Ethernet Host Network 2 and 3 are secondary networks connected to the AirLink device. For example, 192.168.10.0.

Host Network Subnet Mask 2 and Host Network Subnet Mask 3	The subnet for the applicable network. For example, 255.255.255.0, which would with the setting above define a secondary network of 192.168.10.0/24.
Host Network 2 Route and Host Network 3 Route	Indicates what type of router is being used for the host network. If it is a traditional router which handles ARP for addresses on its subnet, select Ethernet. If it is a “dumb” gateway which is a conduit to a subnet but does not handle any ARP, select Gateway. When Gateway is selected, ALEOS will ARP for the destination address and send it to the defined Host Network Gateway address.
Host Network 2 Gateway and Host Network 3 Gateway	The IP address of the 'dumb' Gateway. This should be left as 0.0.0.0 if the Host Network Route is Ethernet. Many routers respond to ARP requests for subnets behind the router. The default is Ethernet, which means that you do not have to configure the gateway IP. For those routers that do not respond to ARP requests for subnets, you need to enter the gateway address.

Wi-Fi

ALEOS provides Wi-Fi configuration capabilities and support for GX Series devices with a Wi-Fi X-Card installed.

This Wi-Fi X-Card works in one of three modes supported in ALEOS:

- Access Point (AP)
- Client
- Both (AP + Client)

Select the Wi-Fi mode to be displayed. The configuration options vary, depending on the mode selected.

Note: Wi-Fi fields appear ONLY if the Wi-Fi X-Card is installed in the AirLink GX Series device.

To configure the Wi-Fi settings:

1. In ACEmanager, go to LAN/WiFi > WiFi.

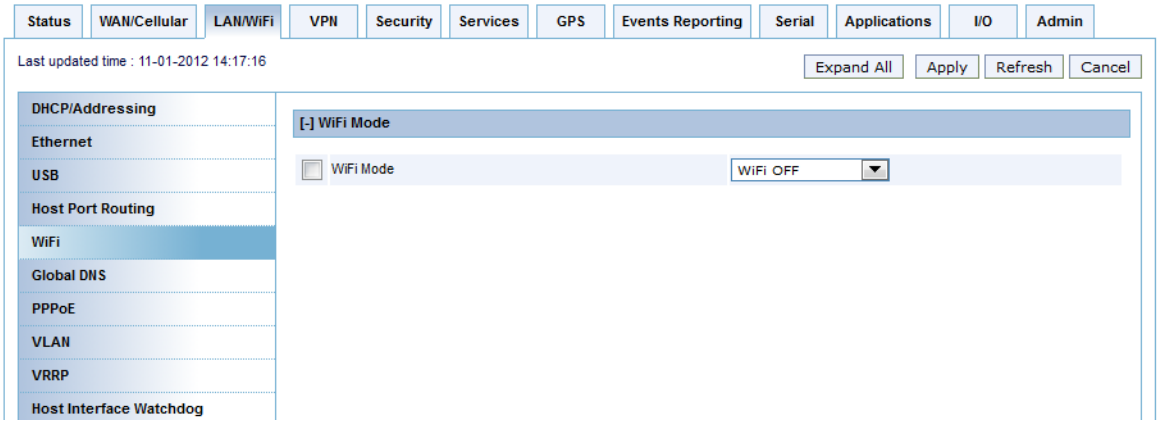


Figure 4-21: ACEmanager: LAN/WiFi > WiFi

Field	Description
Wi-Fi Mode	
WiFi Mode	Allows you to choose the Wi-Fi mode of operation. Options are: • WiFi OFF (Default) • Access Point (See page 86.) • Client Mode (See page 90.) • Both (AP + Client) (See page 92.)

Access Point Mode

In this mode, the AirLink device acts as an access point.

Select Access Point Mode from the drop-down box in the WiFi Mode field, and click “+” beside Access Point to expand that section.

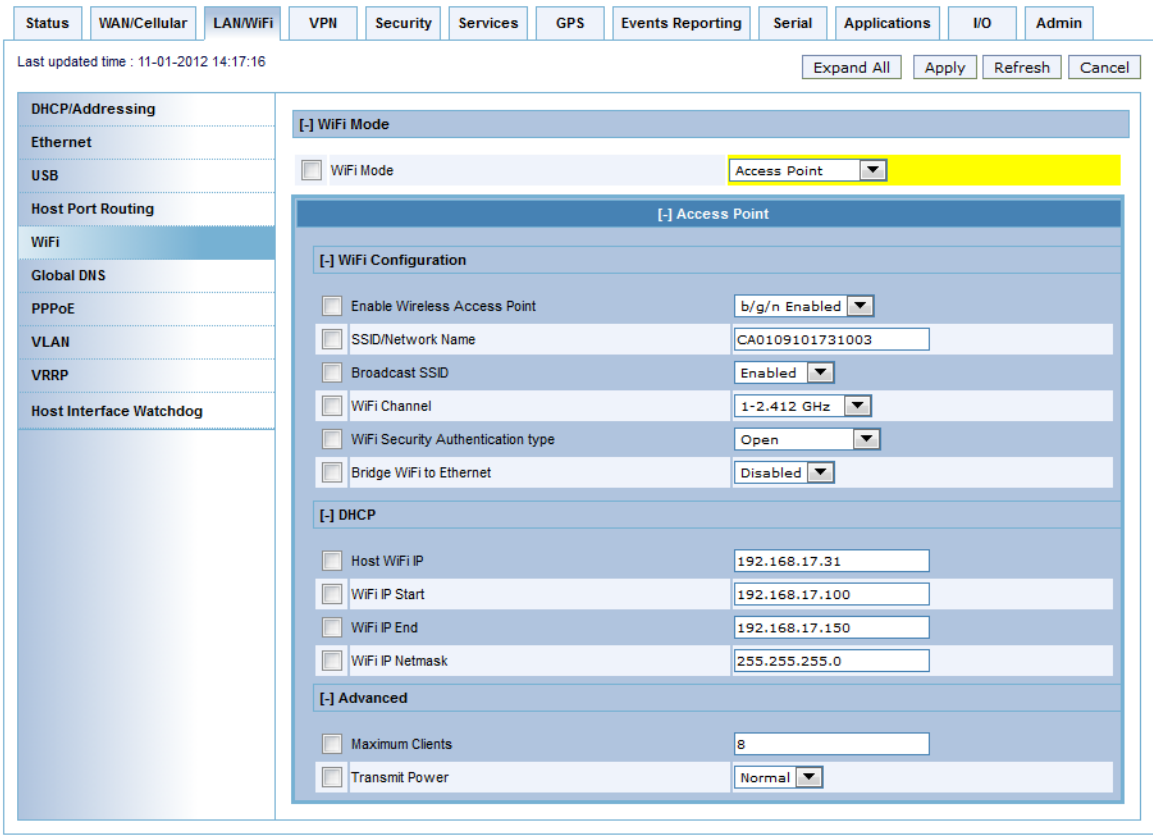


Figure 4-22: ACEmanager: LAN/WiFi > WiFi > Access Point

Field	Description
Wi-Fi Configuration	
Enable Wireless Access Point	Wireless Access Point operation works like an On/Off switch for the Wi-Fi module. When this field is set to disabled, the Wi-Fi module is powered off. The wireless mode configures operation for either 802.11b/g or b/g/n. This field combines both mode and operation into a single configuration item. Options are: • WiFi OFF • b/g Enabled • b/g/n Enabled (Default) *Note: Selecting b/g/n Enabled limits the encryption options to Open and WPA/WPA2.*
SSID/Network Name	You can set the SSID/Network Name or it can be automatically generated (default). The SSID (Service Set Identifier) default value is the same as the AirLink GX Series device serial number which appears on the label on the bottom of the device. Note: Only ONE SSID is available. *Note: The SSID is case-sensitive.*
Broadcast SSID	Suppresses the SSID name in the Wi-Fi Access Point beacon message. Options are: • Enabled (Default) • Disabled
WiFi Channel	This field allows you to select from among 14 Wi-Fi channels. Options begin with Channel 1 at 2.412 GHz, and each subsequent channel increases in frequency by .005 GHz (*except* for Channel 14 which is at 2.484 GHz). Default: 1–2.412 GHz. *Note: Some channels are not available for specific geographical areas.*

WiFi Security Authentication type	This field allows you to select the following authentication Options are:
	• Open—No authentication is needed when this option is selected. This option allows any user to connect to the AP and is generally not recommended. When you select Open, the following options are available:
	  • None (default)
	  • WEP
	• WPA Personal
	• WPA2 Personal
	Note: WEP is not a recommended Wi-Fi Security protocol because of its well publicized vulnerabilities. Use WPA/WPA2 Personal instead. Only alphanumeric characters can be used for the WEP passphrase.

Field	Description
Bridge WiFi to Ethernet	This field allows routing between the Ethernet Lan and WLAN. When enabled, the Ethernet port and the Wi-Fi ports are on the same subnet. Available only when the Wi-Fi has its own subnet (Bridge WiFi to Ethernet is disabled.) Options are: • Enabled (Default) • Disabled
DHCP	
Host WiFi IP	Displays the AP's IP address. Default: 192.168.17.31
WiFi IP Start	Displays the beginning IP address to be served. Default: 192.168.17.100
WiFi IP End	Displays the ending IP address to be served. Default: 192.168.17.150
WiFi IP Netmask	Displays the subnet IP netmask of the WiFi network. When this option is selected, the Wi-Fi cannot be bridged to Ethernet. Default: 255.255.255.0
Advanced	
Maximum Clients	Indicates the maximum number of concurrent users (clients) to be supported. The administrator specifies this number which can range from 1 to 8. Default: 8.
Transmit Power	Adjusts the transmit power of the AP. Options are: • High—High Power (16 dB) Default • Low—Low Power (10 dB)

When the b/g Enabled option is selected from the Enable Wireless Access Point field's drop-down menu, and Open is selected in the WiFi Security Authentication type field, an additional section for Open WEP appears:

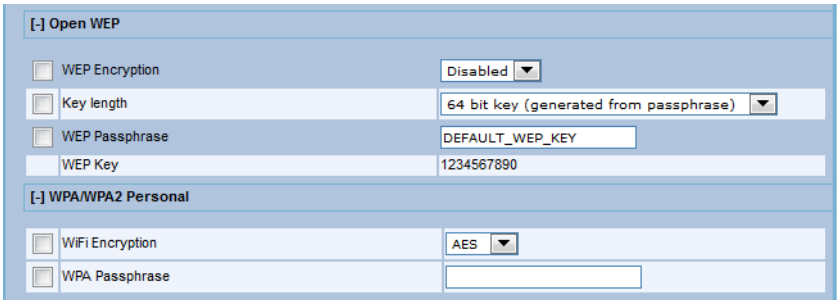


Figure 4-23: ACEmanager: LAN/WiFi > Access Point Open WEP section

Field	Description
Open WEP	
Note: WEP is not a recommended Wi-Fi Security protocol because of its well publicized vulnerabilities. Use WPA/WPA2 Personal instead. Only alphanumeric characters can be used for the WEP passphrase. WEP is only available if the Enable Wireless Access Point field is set to b/g Enabled. (See Enable Wireless Access Point on page 87.)	
WEP Encryption	If Enabled is selected, the following three fields in this table display. Options are: Enabled or Disabled
Key length	Options are: • 64 bit key (generated from password)—Default • 128 bit key (generated from password) • 64 or 128 bit key (customer specifies 5 or 10 hex characters)
WEP Passphrase	May be 10–255 alphanumeric ASCII characters long. This field is not used if the 64 or 128 bit key (customer) option is selected in the Key length field.
WEP Key	Displays the WEP key in hex characters The WEP Key is generated from the WEP Passphrase when the Key length is 64-bit key or 128-bit key. This is the Key required by AP clients to connect to the device. To generate the WEP Key: **1.** Set the Key length. **2.** Enter the WEP Passphrase. **3.** Click Apply. **4.** Reboot the device.

If WPA Personal or WPA2 Personal are selected for the WiFi Security Authentication type field, a WPA/WPA2 Personal section replaces the Open WEP section in the user interface.

Field	Description
WPA/WPA2 Personal	
WiFi Encryption	Specify the encryption type for WPA or WPA2 authentication. Options are: • TKIP—Available for 802.11b/g, not available for 802.11n. • AES (default) *Note: If WPA2 is selected as the authentication type (see WiFi Security Authentication type on page 87) only AES is available.*
WPA Passphrase	Specify the length of the WPA Passphrase AP clients use to connect to the device. Minimum length is 8 characters and maximum length is 64. Default: None.

Client Mode

Client Mode allows a mobile AirLink GX Series device to use a Wi-Fi Client connection to connect to an access point, rather than acting as an access point.

Client Mode has been tested with the top 5 WLAN Access Point vendors: Cisco®, Aruba Networks®, Motorola™, HP®, and NETGEAR®.

You can configure up to 8 Access Points for each AirLink GX Series device. Only one Access Point is used at a time for the client connection. Having additional APs configured allows for portability.

Select Client Mode from the drop-down box in the WiFi Mode field, and click “+” beside Client Mode to expand that section.

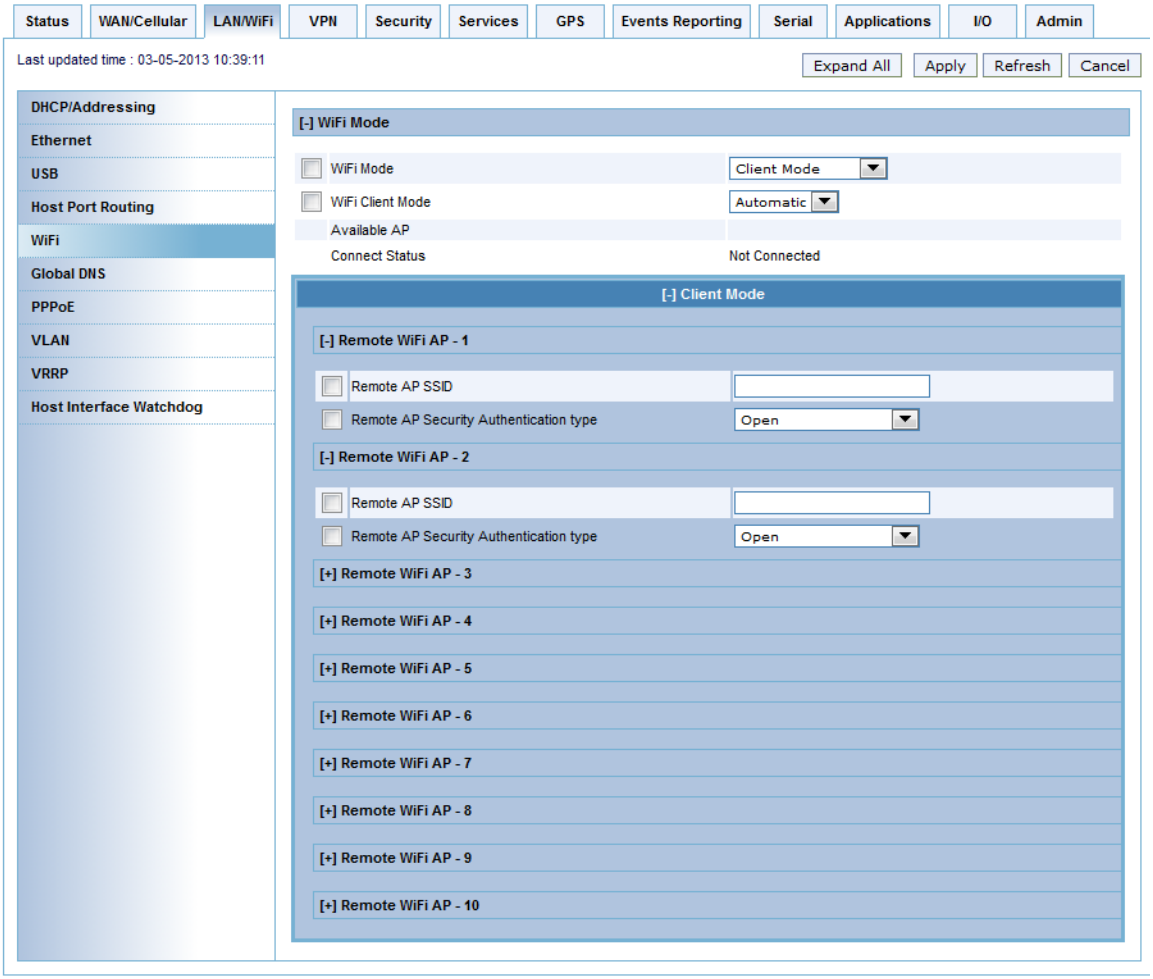


Figure 4-24: ACEmanager: LAN/WiFi > WiFi > Client Mode > Automatic

Field	Description
WiFi Mode	
WiFi Client Mode	Allows you to choose the connection mode type. Options are: • Automatic (default)—the WAN connection automatically switches from cellular to Wi-Fi whenever the Wi-Fi connection has been established • Manual To connect in manual mode: **1.** Open ACEview and go to Menu > View > Wi-Fi. **2.** ACEview displays a list of available access points. and the connection state. **3.** Select an available AP, and click Connect. A message window appears asking if you wish to connect the available Access Point. **4.** Click OK. *Note: Whenever changing the Wi-Fi Client Mode from Automatic to Manual or Manual to Automatic, you must reboot the device.*
Available AP	Identifies the currently available access point Only one AP is shown, even if additional ones are configured. If there is more than one AP available in the area, the one that is highest in the configuration order (in the ACEmanager) is displayed.

Field	Description
Connect	This button only appears when the Manual WiFi Client Mode is selected. Select to activate the Manual mode.
Connect Status	Indicates whether the WiFi Client Mode is connected or not connected
Remote WiFi AP - 1, Remote WiFi AP - 2, and Remote WiFi AP - 3	
Remote AP SSID	You can set the SSID/Network Name or it can be automatically generated (default). The SSID (Service Set Identifier) default value is the same as the AirLink GX Series device serial number that appears on the label on the bottom of the device. Note: Only one SSID is available. *Note: The SSID is case-sensitive.*
Remote AP Security Authentication type	Select the appropriate authentication type for the access point the device is connecting to. Options are: • Open—No authentication is needed when this option is selected. This option is generally not recommended since it offers no authentication or encryption. Default. • WPA/WPA2 Personal • WEP *Note: WEP is not a recommended Wi-Fi Security protocol because of its well publicized vulnerabilities. WPA/WPA2 Personal is recommended. Only alphanumeric characters can be used for the WEP passphrase.*
Remote AP WPA Passphrase	Specifies the remote AP WPA Passphrase. Minimum length is 8 characters, and maximum length is 64 characters.

Both (AP + Client) Mode

In this mode, the AirLink GX Series device can act as an access point and also use a Wi-Fi Client connection to connect to an access point. The AirLink GX Series device connects as a client to a configured Access Point (AP) whenever the AP is available, when the AP is not available, it connects to the cellular network, all the while the AirLink GX Series device is acting as a AP to W-Fi clients connected to the GX.

When you select this mode from the WiFi Mode drop-down menu, you can configure the Access Point and Client fields on one window. (Click “+” beside each section to expand it.)

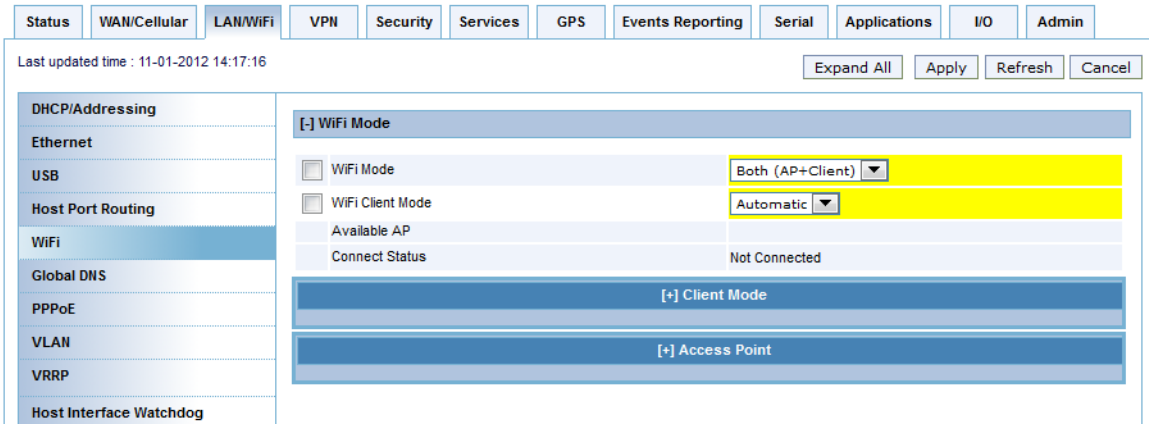


Figure 4-25: ACEmanager: LAN/WiFi > WiFi > Both (AP + Client) Mode

For information on configuring the required fields, see Access Point Mode on page 86 and Client Mode on page 90.

Global DNS

When the cellular network grants the IP address to the device, it includes the IP addresses to its DNS servers. Global DNS allows you to override the carrier's DNS settings for all connected devices. This is useful when the connected devices need to use a private network.

Note: If there are no alternate DNS defined, the default is the cellular network DNS sever.

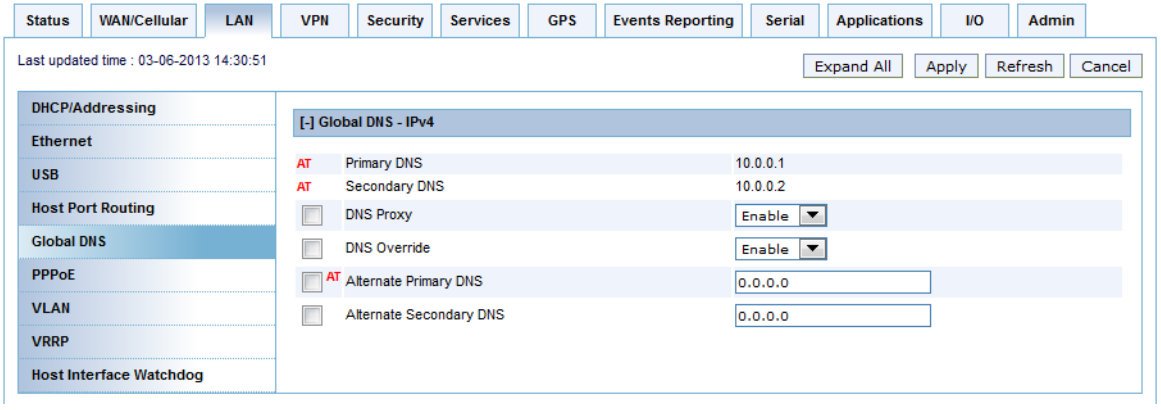


Figure 4-26: ACEmanager: LAN > Global DNS

Field	Description
Primary DNS	Primary carrier DNS IP Address. This and the secondary DNS are generally granted by the cellular network along with the Network IP.
Secondary DNS	Secondary carrier DNS IP Address

Field	Description
DNS Proxy	Determines how the connected hosts acquire their first DNS server. Options are: • Enable (default) —All connected hosts (PPP, PPPoE, Wi-Fi, USBNET, and Ethernet) acquire the AirLink device's IP address as the first DNS server and use the AirLink device as their DNS resolver. • Disable—All connected hosts acquire the Mobile Network Operator-defined DNS server as the first DNS server. The AirLink device is not used as the DNS resolver.
DNS Override	Overrides the carrier DNS addresses with user configured ones. Some carriers ignore the use of Alternate DNS servers and route all DNS requests to their own servers. Options are: Disable (default) or Enable.
Alternate Primary DNS	Configurable DNS server to use instead of the cellular network-granted one
Alternate Secondary DNS	Configurable DNS server to use instead of the cellular network-granted one

PPPOE

PPPoE (Point-to-Point Protocol over Ethernet) allows a point-to-point connection while using Ethernet. Just like the dial up protocol on which it is based, PPPoE can use traditional user name and password authentication to establish a direct connection between two Ethernet devices on a network (e.g., your AirLink device and your computer or router).

Application examples for PPPoE with your AirLink device:

- Backup connectivity solution for your network
- Individualized Internet connection on a LAN
- Password restricted Internet connection

Only one computer, router, or other network device at a time can connect to the AirLink device using PPPoE. If you are using the AirLink device connected to a router as a back up Internet connection for your network, you should configure the router to use the PPPoE connection and not the individual computers.

Note: To configure a PPPoE connection on some operating systems, you need administrator privileges to the computer you are configuring or access granted by an administrator on the network to add/remove devices to your computer.

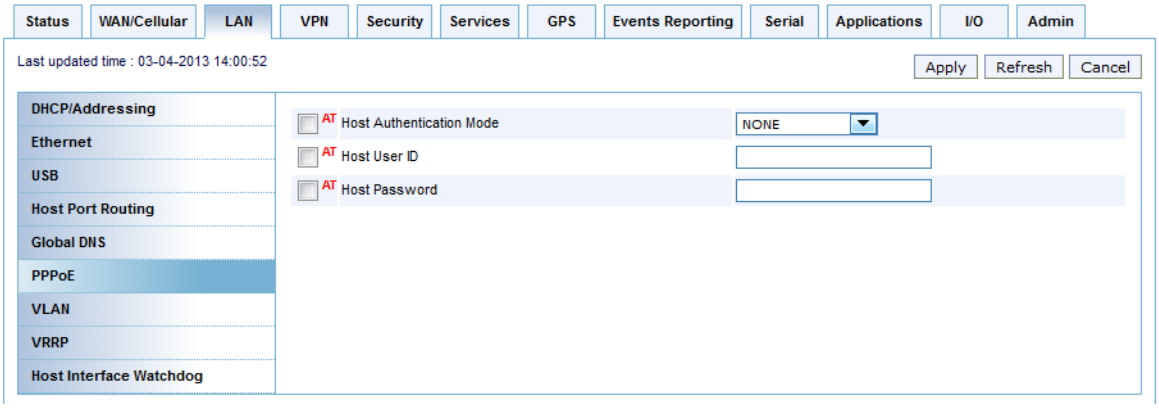


Figure 4-27: ACEmanager: LAN > PPPoE

Field	Description
Host Authentication Mode	Host Authentication Mode: Use PAP or CHAP to request the user login and password during PPP or CHAP negotiation on the host connection. The username and password set in *HOSTUID and *HOSTPW is used. • NONE (Default) • PAP and CHAP • CHAP
Host User ID	User ID for authentication (up to 64 bytes)
Host Password	Password for authentication

Configure the AirLink Device to Support PPPoE

Note: You must disable the DHCP server for PPPoE to work.

To configure an AirLink device to support PPPoE:

1. In ACEmanager, go to LAN > Ethernet.
2. Under General, in the DHCP Server Mode filed, select Disable.

Note: PPPoE authentication is optional. If you use PPPoE authentication, no other tethered LAN connection will have network access, regardless of whether or not the PPPoE host is connected. If you are using non-authenticated PPPoE, other tethered LAN connections will have network access until a PPPoE host is connected.

3. If you want to use authenticated PPPoE:
   a. Go to LAN > PPPoE, and in the Host Authentication Mode field, select PAP and CHAP.
   b. In the Host User ID, enter a user ID for the PPPoE connection.

c. In the Host Password field, enter a password for the PPPoE to connection.

4. Click Apply.
5. Reboot the device.

Tip: *If you leave Host User ID and Host Password blank, any computer or device can connect to the AirLink device using PPPoE.*

Note: ACEmanager shows the existing value for the PPPoE password as stars (****).

Optional: Configure the Device Name

1. In ACEmanager, go to Services > Dynamic DNS.
2. In the Service field, select IP Manager.
3. Under Dynamic IP, enter a name in the Device Name field, such as AirLink device or the ESN. The name can be up to 20 characters long.

   The name you choose for Device Name does not affect the connection, but may need to be configured in PPPoE settings for the router, device, or computer you connect to your AirLink device.

Configuring a PPPoE Connection in Windows 7

1. In Windows 7, go to Start > Control Panel.

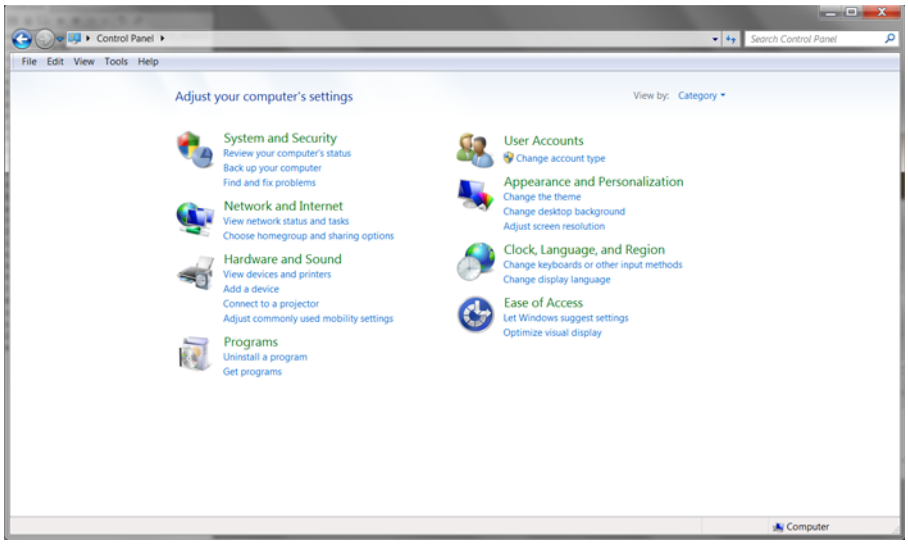


Figure 4-28: Windows 7: Control Panel

2. Select Network and Internet.

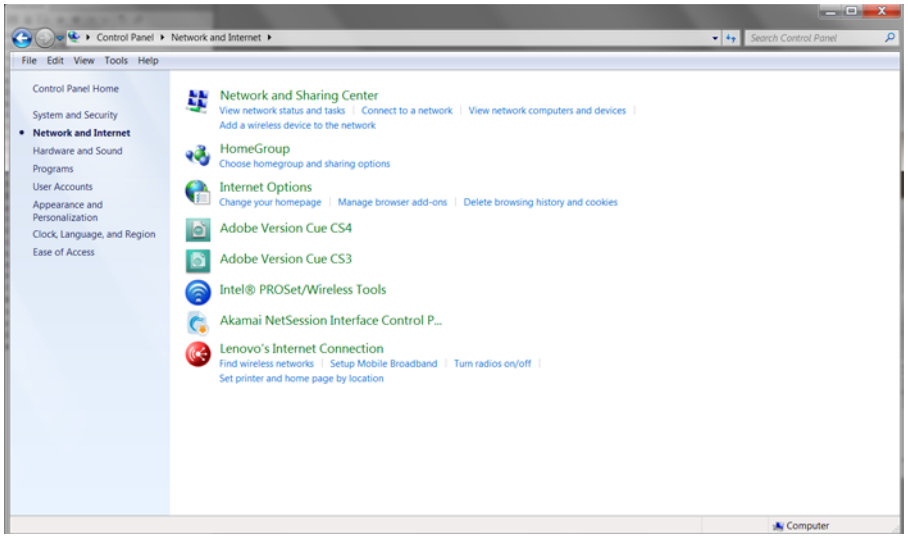

Control Panel ▸ Network and Internet ▸
Search Control Panel
File Edit View Tools Help
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts
Appearance and Personalization
Clock, Language, and Region
Ease of Access
Network and Sharing Center
View network status and tasks | Connect to a network | View network computers and devices
Add a wireless device to the network
HomeGroup
Choose homegroup and sharing options
Internet Options
Change your homepage | Manage browser add-ons | Delete browsing history and cookies
Adobe Version Cue CS4
Adobe Version Cue CS3
Intel® PROSet/Wireless Tools
Akamai NetSession Interface Control P...
Lenovo's Internet Connection
Find wireless networks | Setup Mobile Broadband | Turn radios on/off
Set printer and home page by location
Computer

Figure 4-29: Windows 7: Control Panel > Network and Internet

3. Select Network and Sharing Center.

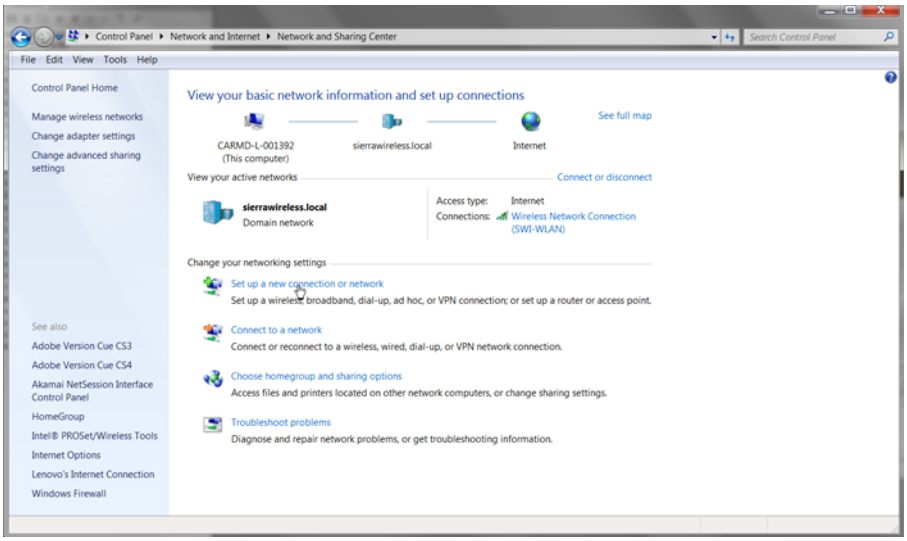

Control Panel ▸ Network and Internet ▸ Network and Sharing Center
Search Control Panel
File Edit View Tools Help
Control Panel Home
Manage wireless networks
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
CARMD-L-001392
(This computer)
sierrawireless.local
Internet
View your active networks
Connect or disconnect
sierrawireless.local
Domain network
Access type: Internet
Connections: Wireless Network Connection (SWI-WLAN)
Change your networking settings
Set up a new connection or network
Set up a wireless broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.
Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.
See also
Adobe Version Cue CS3
Adobe Version Cue CS4
Akamai NetSession Interface Control Panel
HomeGroup
Intel® PROSet/Wireless Tools
Internet Options
Lenovo's Internet Connection
Windows Firewall

Figure 4-30: Windows 7: Control Panel > Network and Sharing Center

4. In the middle of the page, under Change your networking settlings, select Set up a new connection or network.

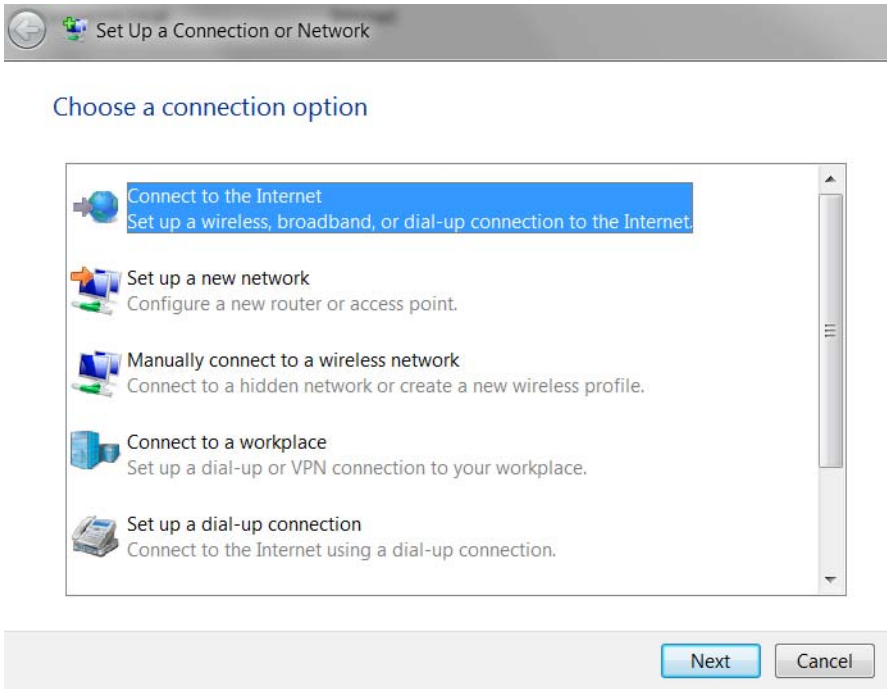
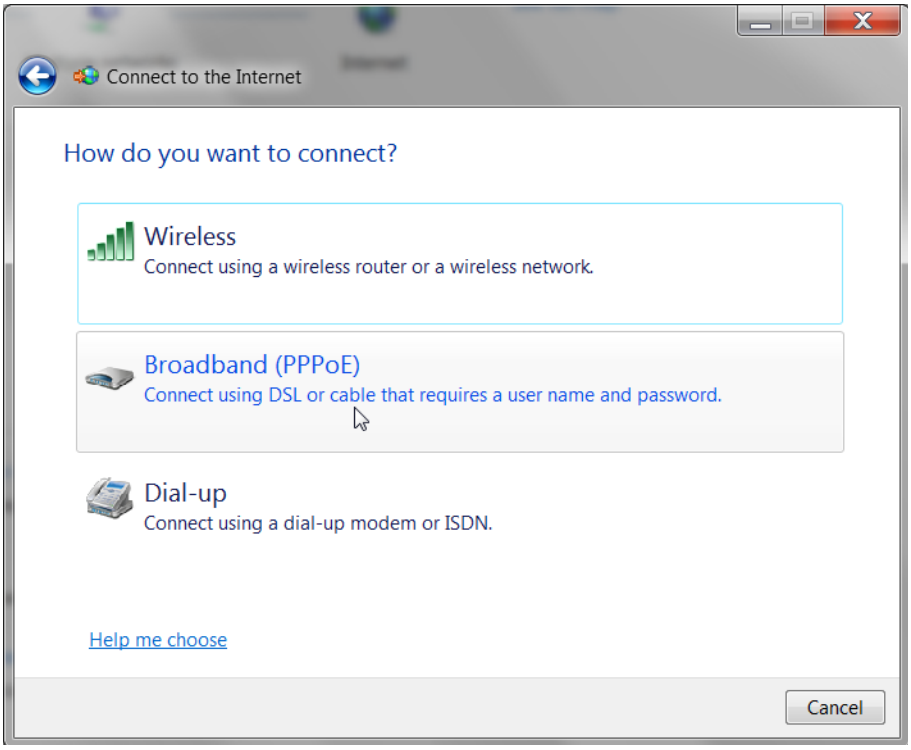
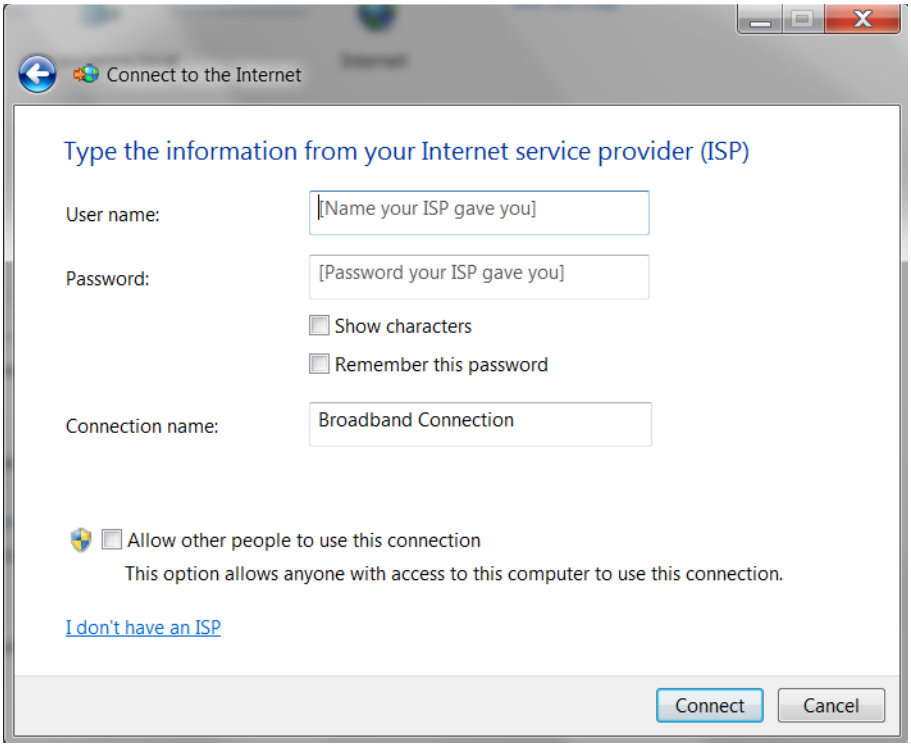

Set Up a Connection or Network
Choose a connection option
Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.
Set up a new network
Configure a new router or access point.
Manually connect to a wireless network
Connect to a hidden network or create a new wireless profile.
Connect to a workplace
Set up a dial-up or VPN connection to your workplace.
Set up a dial-up connection
Connect to the Internet using a dial-up connection.
Next
Cancel

Figure 4-31: Set Up an Connection or Network

5. Select Connect to the Internet and click Next.


Connect to the Internet
How do you want to connect?
Wireless
Connect using a wireless router or a wireless network.
Broadband (PPPoE)
Connect using DSL or cable that requires a user name and password.
Dial-up
Connect using a dial-up modem or ISDN.
Help me choose
Cancel

6. Select Broadband (PPPoE).


Connect to the Internet
Type the information from your Internet service provider (ISP)
User name:
[Name your ISP gave you]
Password:
[Password your ISP gave you]
Show characters
Remember this password
Connection name:
Broadband Connection
Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.
I don't have an ISP
Connect
Cancel

7. If you are using authenticated PPPoE, enter the User name and Password you configured in ACEmanager.
8. If desired, change the Connection name to something such as PPPoE that clearly identifies the connection.
9. Click Connect.

For subsequent connections, you can click the network icon in the Task bar ( ) and select the PPPoE connection.

VLAN

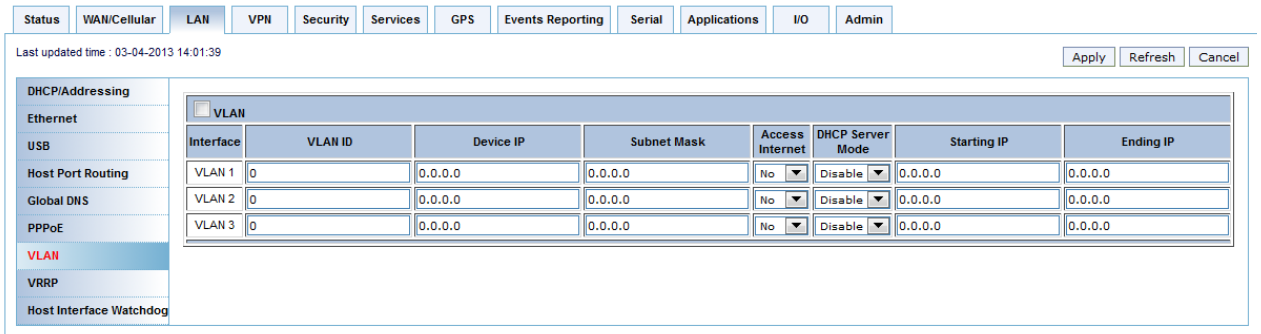


Figure 4-32: ACEmanager: LAN > VLAN

Field	Description
Interface	Displays three VLAN IDs
VLAN ID	Displays the VLAN ID
Device IP	The IP address of the AirLink device for that VLAN interface
Subnet Mask	The subnet mask indicates the range of host IP addresses which can be reached directly. Changing this limits or expands the number of clients that can connect to the AirLink device.
Access Internet	Choose access to the Internet. Scroll down options are: “Yes” or “No.”
DHCP Server Mode	Options are Enable and Disable (default)
Starting IP	VLAN interface DHCP pool starting IP address
Ending IP	The ending IP for the VLAN interface

VRRP

VRRP (Virtual Router Redundancy Protocol) allows multiple routers to act as the default gateway router for a subnet, thereby reducing the possibility of a single point of failure.

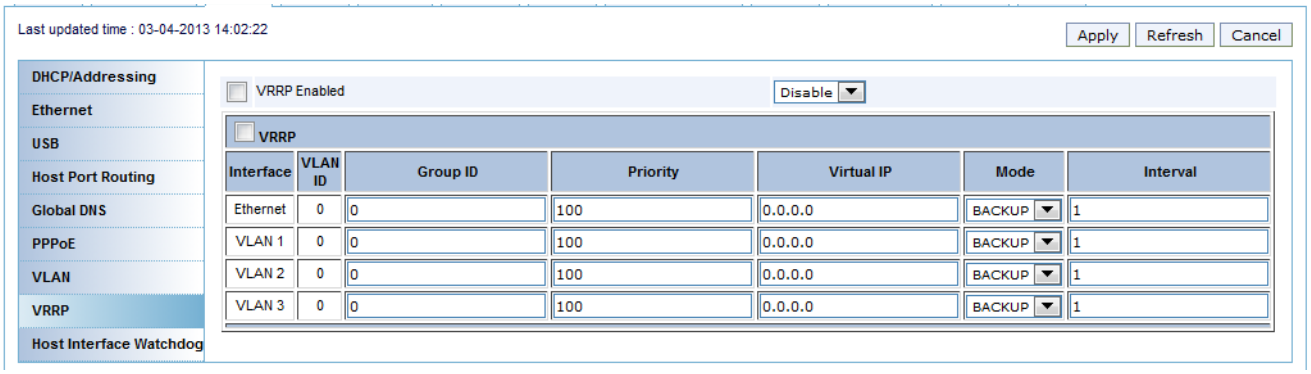


Figure 4-33: ACEmanager: LAN > VRRP

Field	Description
VRRP Enabled	Allows you to activate VRRP. Options are: • Enable • Disable (default)
VRRP	
Interface	Displays Ethernet and three VLAN IDs
VLAN ID	Displays the VLAN ID

Field	Description
Group ID	Enter the VRRP Group ID. VRRP routers in the master and slave have the same Group ID.
Priority	VRRP decides whether the device is the master or slave. A greater value of priority indicates that the device is the master.
Virtual IP	If a device is configured with VRRP, the host connected to the device displays the Virtual ID. Virtual IP becomes the VRRP router's Device IP.
Mode	Indicates whether the device is MASTER or BACKUP (default). The Priority number determines the master or backup status
Interval	VRRP advertised interval; Default: 1 second

Host Interface Watchdog

The Host Interface Watchdog provides a way for you to ensure that the LAN connection is alive. You can use this feature to monitor:

- A host connected to the LAN via an Ethernet or USB connection
- A host computer associated with a GX Series device that has a Wi-Fi X-Card installed, provided the Wi-Fi mode is set to "Access Point" or "Both" (See Wi-Fi on page 85.)

When the Host Interface Watchdog is enabled, ALEOS sends a ping to the connected host at configured intervals. You can disable Force Keepalive to only send a ping when there is no traffic on the LAN interface. (See Force Keepalive on page 102.)

If there is no response to the ping, the LAN interface is reset.

Note: The network interface is automatically determined from the IP address and the LAN configuration. If you have multiple interfaces bridged (see Bridge WiFi to Ethernet on page 72) all interfaces in the bridge and the bridge itself are reset.

After the interface comes back up, ALEOS sends another ping to the connected host. If there is still no response to this ping, the AirLink device reboots. After a reboot caused by the LAN Interface Watchdog, ALEOS waits an hour before attempting pings to prevent repeated frequent reboots.

Note: DUN (PPP) is not supported. If the IP address for the host is on a DUN network, the feature is disabled.

Note: The feature is not disabled when the interface uses Public Mode, but it cannot monitor the host interface unless the cellular network provides a static IP.

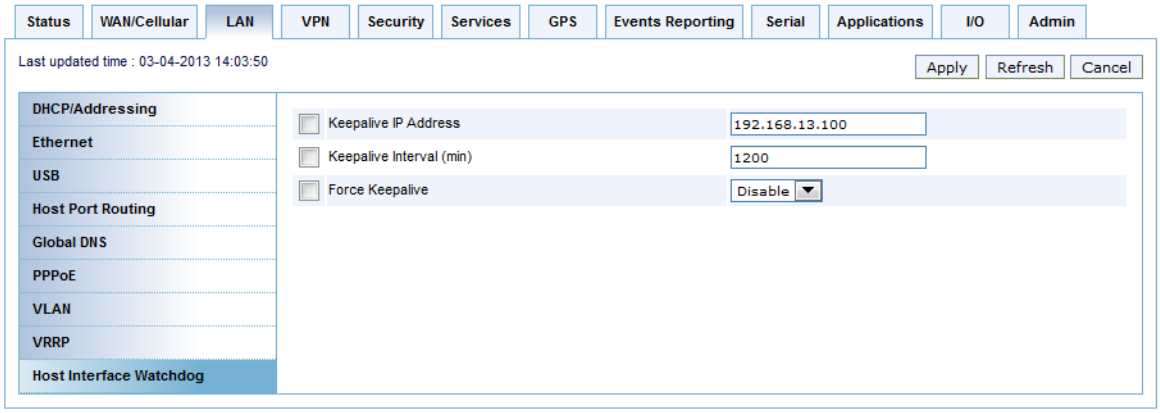


Figure 4-34: ACEmanager: LAN > Host Interface Watchdog

Field	Description
Keepalive IP address	Enter the IP address of the host to ping If a host IP address is not configured, the Host Interface Watchdog is disabled.
Keepalive Interval (min)	The interval (in minutes) at which ALEOS pings the LAN-connected device Options are: 1–1440 If this field is set to 0, the Host Interface Watchdog is disabled. (default)
Force Keepalive	• Enabled (default)—The network interface statistics are not monitored and a ping is always sent at the interval configured in the Keepalive Interval field. • Disabled—The network interface statistics are monitored and connectivity is assumed when there is traffic received. A ping is only sent when there is no traffic for a period greater than the interval set in the Keepalive Interval field.

5: WAN/Cellular Configuration

5

The WAN/Cellular section allows changes to the cellular connection and main operating mode of the AirLink device. The options available in ACEmanager depend on the type of technology your AirLink device use. Refer to the appropriate section for your device:

- CDMA
- GSM on page 106
- LTE—Fallback to EV-DO on page 111
- LTE—Fallback to HSPA+ on page 113

CDMA

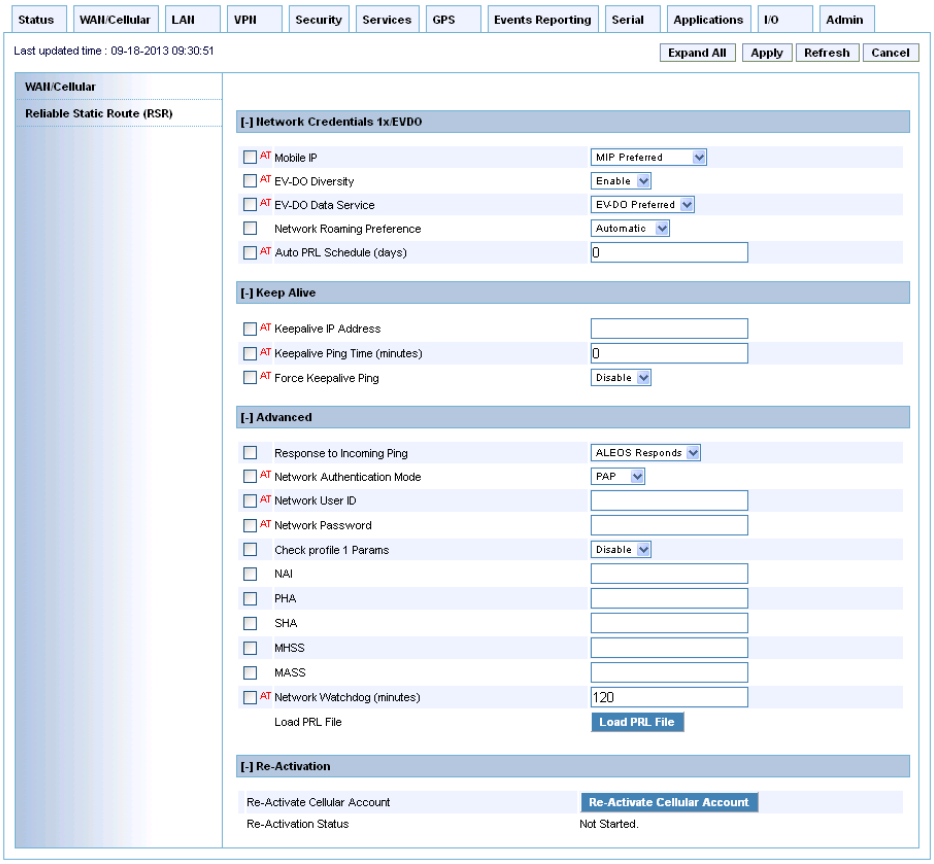


Figure 5-1: ACEmanager: WAN/Cellular —1x/EV-DO

Command	Description
Network Credentials 1x/EVDO	
Mobile IP	Mobile IP (MIP) Preferences. On a Mobile IP network, a device connects to the network using PPP. During the negotiation process the AirLink device is NOT required to present a username and password to authenticate because the authentication parameters are stored in the device itself. • Disabled, SIP only • MIP Preferred • MIP Only Default: MIP is used when available with a fall back to SIP. *Note: Your account with your Mobile Network Operator may not support all three of these options. check with your Mobile Network Operator as to which one should be used.*
EV-DO Diversity	EV-DO Diversity allows two antennas to provide a more consistent connection. • Disable • Enable (default) If you are not using a diversity antenna, diversity should be disabled. *Note: This field is not available in all AirLink devices.*
EV-DO Data Service	Change the allowable network type: • EV-DO Preferred — can “fall back” on CDMA/1x • EV-DO Only — fall back disabled • 1x Only — EV-DO disabled *Note: For most users, it’s best to leave the default setting (EV-DO Preferred). When this option is selected, your AirLink device connects to an EV-DO network if it is available and falls back to a CDMA 1x network if EV-DO service is not available. If you choose another option and the selected network is not available, the device will not be able to connect to the cellular network. For example, if you select EV-DO Only and you are in an area where there is no EV-DO network available, the device will not be able to connect to a cellular network until you change this setting.*
Network Roaming Preference	Allows you to control whether or not roaming (connecting to a mobile broadband network other than that of your Mobile Network Operator). Options are: • Automatic—The device connects to the home network if it is available and to another Mobile Network Operator’s network if the home network is not available (for example you are outside the coverage area). Note: Roaming charges may apply. • Home Only—The device only connects to the home network. If the home network is not available (for example, if you are outside the coverage area) the device does not connect until the home network is available again.
Auto PRL Schedule (days)	Indicates the PRL update schedule • 0=disable
Keep Alive (See Keepalive on page 116.)	

Command	Description
Advanced	
Response to Incoming Ping	When a ping is received by the device from a remote location, the Response to Incoming Ping redirects it to the selected location. • No response: the incoming ping is completely ignored • ALEOS Responds (default): ALEOS returns to the Ping response. • Pass to Host: The ping is forwarded to the DMZ host with any response from the host forwarded back to the OTA location. If no host is connected, there is no ping response. *Note: Some Mobile Network Operators may block all ICMP traffic on their network. A ping sent to the device from a remote location is not received.*
Network Authentication Mode	Specifies the authentication method to use in the network PPP session. Options are: • None • CHAP • PAP (default)
Network User ID	Network User ID The login that is used to login to the cellular network, when required. • uid=user id (up to 64 bytes)
Network Password	Network Password is the password that, when required, is used to login to the cellular network. pw=password (30 characters maximum).
Check profile 1 Params	Enables checking and updating the Profile 1 Parameters. Options are: • Enable • Disable (default) *Not all Mobile Network Operators or account types support this feature.*
NAI	Sets the Network Access ID Not all Mobile Network Operators or account types support this feature.
PHA	Sets the IP address of the primary home agent Not all Mobile Network Operators or account types support this feature.
SHA	Sets the IP address of the secondary home agent Not all Mobile Network Operators or account types support this feature.
MHSS	Sets the home agent shared secret key Not all Mobile Network Operators or account types support this feature.
MASS	Sets the AAA shared secret key Not all Mobile Network Operators or account types support this feature.
Network Watchdog (minutes)	Network connection watchdog If there is no WWAN/Cellular network connection for the number of minutes configured in this field, the device reboots. This feature cannot be disabled. • 5–255 minutes (allowed values) • 120 minutes (default)
Load PRL File	The Load PRL File button allows you to download a Preferred Roaming List.
Update PRL	The Update PRL button allows you to update your Preferred Roaming List.

Command	Description
Update Profile	The Update Profile button allows you to update the profile of your Preferred Roaming List.
Re-Activation	
Re-Activate Cellular Account	See Re-Activation on page 118.
Re-Activation Status	See Re-Activation on page 118.

GSM

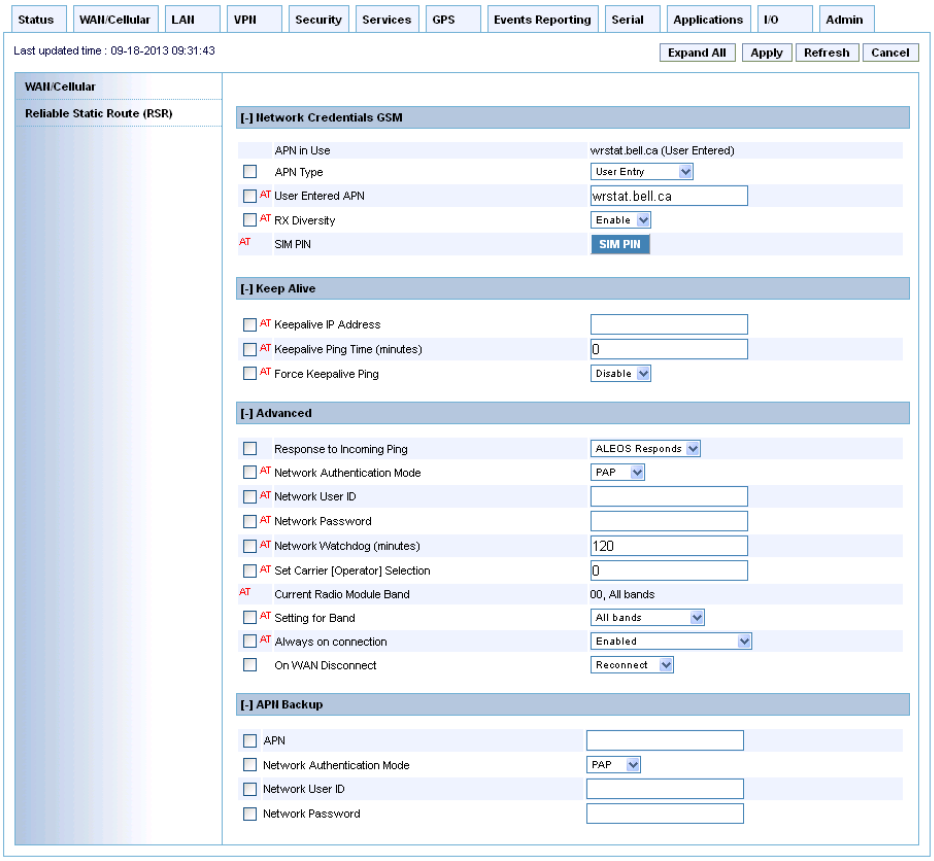
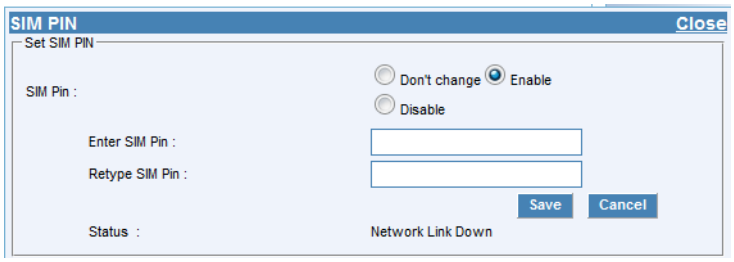


Figure 5-2: ACEmanager: WAN/Cellular—GSM

Command	Description
Network Credentials GSM	
APN in Use	The APN in use for the current cellular connection.

Command	Description
APN Type	Choose to use an APN based on the SIM in use or a custom APN manually entered. • Select From List — When selected, a list of APNs based on the SIM in use are available as a drop-down list. • User Entry — When selected, an entry field appears for typing in the APN that should be used
User Entered APN	Displays if the APN type is "User Entry." Enter the APN of your choice.
RX Diversity	Allows two antennas to provide a more consistent connection • Disable • Enable (default) If you are not using a diversity antenna, diversity should be disabled. *Note: This field is not available in all AirLink devices.*
SIM PIN	If your AirLInk device has a PIN-locked SIM card installed, before the device goes on-air for the first time: **1.** Obtain the PIN from your Mobile Network Operator. **2.** Click the SIM PIN button.  **3.** Select Enable. **4.** Enter the PIN twice and click Save. *Note: On subsequent reboots and reconnects, ALEOS automatically uses the PIN. This feature prevents the SIM from being used in another device without re-entering the PIN.* *Note: You have three attempts to enter the correct PIN. If the correct PIN is not entered by the third attempt, the SIM card becomes blocked and you need a PUK code from your Mobile Network Operator to unlock it. For more information, see SIM Card is Blocked on page 397.*
Keep Alive (See Keepalive on page 116.)	

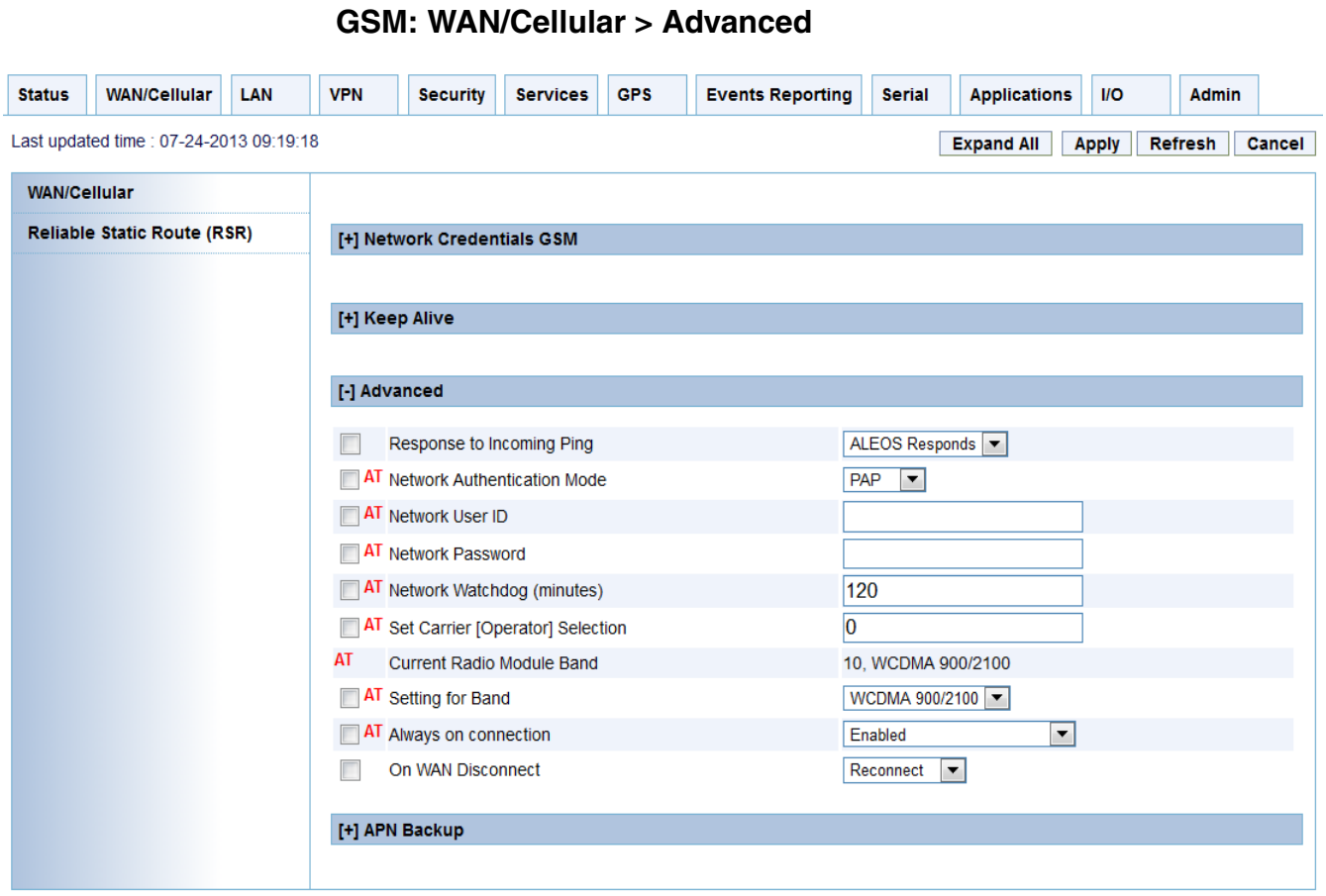


Figure 5-3: ACEmanager: WAN/Cellular > Advanced

Field	Description
Response to Incoming Ping	When a ping is received by the device from a remote location, the Response to Incoming Ping redirects it to the selected location. • No response: the incoming ping is completely ignored • ALEOS Responds (default): ALEOS returns to the Ping response. • Pass to Host: The ping is forwarded to the DMZ host with any response from the host forwarded back to the OTA location. If no host is connected, there is no ping response. *Note: Some Mobile Network Operators may block all ICMP traffic on their network. A ping sent to the device from a remote location is not received.*
Network Authentication Mode	Specifies the authentication method to use in the network PPP session. Options are: • None • CHAP • PAP (default)

Field	Description
Network User ID	Network User ID The login that is used to login to the cellular network, when required. • uid=user id (up to 64 bytes)
Network Password	Network Password is the password that, when required, is used to login to the cellular network. pw=password (30 characters maximum).
Network Watchdog (minutes)	Network connection watchdog If there is no network connection for the number of minutes configured in this field, the device reboots. This feature cannot be disabled. • 5–255 minutes (allowed values) • 120 minutes (default)
Set Carrier (Operator) Selection	Manually specify an operator. Enter the desired parameters in the following format: mode[,format[,oper]] • mode= 0: Automatic — any affiliated carrier [default] • mode= 1: Manual — use only the operator <oper> specified • mode= 4: Manual/Automatic — if manual selection fails, goes to automatic mode • format= 0: Alphanumeric (“name”) • format= 2: Numeric • oper=”name” See also to +COPS and *NETOP? *Note: Not all carriers or accounts allow specifying the operator. If the carrier doesn't support it, this command may appear to be ineffectual.*
Current Radio Module Band	Band reported by the radio module.
Setting for Band	This feature enables advanced users to select the RF band range or technology the AirLink device uses. Most of the time it’s best to leave this field at the default setting (All bands) but there may be times when you want to select a band range or technology that you know is more stable in the region where the AirLink device is located. The list of options displayed depends on the radio module in your device and its configuration. Possible options include: • All bands (default) • GSM 900/1800 • GSM ALL • WCDMA ALL • WCDMA 900/2100 *Note: For some Mobile Network Operator SIM Cards, you may need to set the radio band before installing the SIM card.*

Field	Description

Always on connection	This option allows you to configure the AirLink device to use minimal wireless network resources when there has not been any outgoing WAN network traffic.
	• Enabled—The AirLink device maintains a mobile network data connection. (default)
	• Disabled—Connect on traffic—The AirLink device only establishes a mobile network data connection:
	  • When there is network traffic
	  • If SMS Wakeup is configured and the device receives the specified type of SMS (For information on configuring SMS Wakeup, see SMS Wakeup on page 168.)
	*Note: You can also use AT*RADIO_CONNECT to switch the cellular network connection on and off. See *RADIO_CONNECT on page 333.*

Connection timeout (minutes)	This field defines the timeout period for Always on connection, and is only visible when Always on Connection is set to Disabled - Connect on traffic. If there is no outgoing packet through the WAN interface during the period set in this field (in minutes), the AirLink device disables the WAN connection. This timer is triggered after every outgoing packet, except AT*IPPINGFORCE keep alive packets. • 2–65535 minutes (Default is 2.) *Note: You can also use AT*TRAFWUPTOUT to set the timeout period. See *TRAFWUPTOUT on page 334.*
On WAN Disconnect	If a disconnect from the Mobile Network Operator occurs: • Reconnect (default) • Reset Radio — ALEOS resets the radio after a Mobile Network Operator disconnect.
APN Backup (See Backup APN on page 119.)	

LTE—Fallback to EV-DO

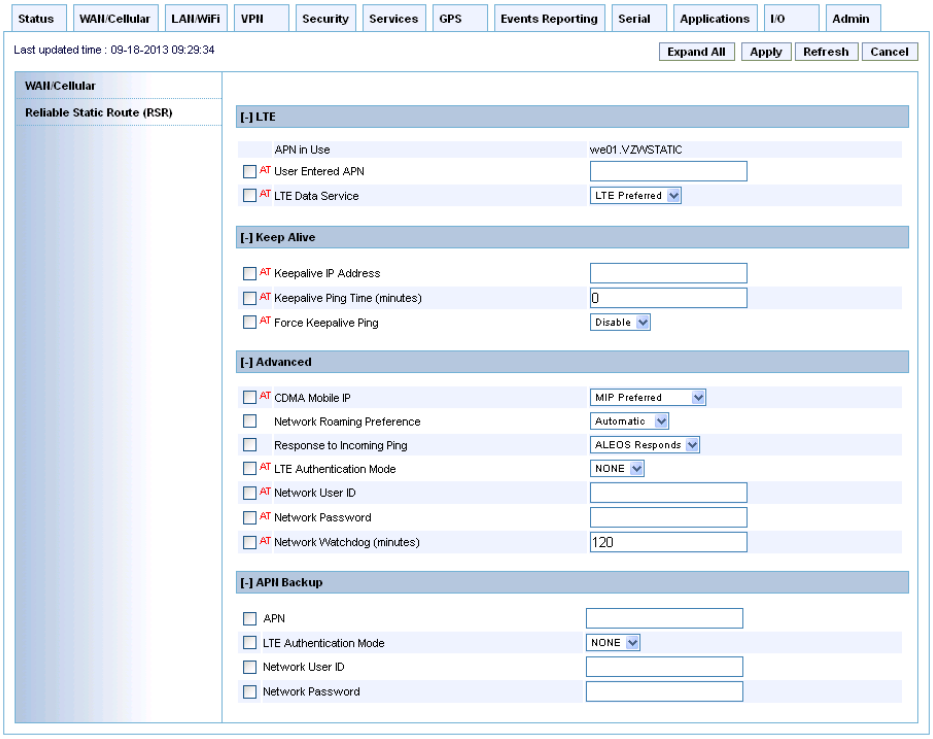


Figure 5-4: ACEmanager: WAN/Cellular > LTE - Fallback to EV-DO

Command	Description
LTE (falls back to EV-DO)	
APN in Use	The APN in use for the current cellular connection
User Entered APN	Enter the desired APN. *Note: If you are activating a GX440 device using a SIM card for an account with special properties, such as a static IP APN, on the LTE network:* **1.** *Enter the static IP APN in this field.* **2.** *Click Apply.* **3.** *Click Reboot.*

Command	Description
LTE Data Service	For LTE, fallback to EV-DO networks. Options are: • LTE Preferred (default)—EV-DO is used when LTE service is not available • CDMA Only • LTE Only *Note: For most users, it's best to leave the default setting (LTE Preferred). When this option is selected, your AirLink device connects to an LTE network if it is available and falls back to an EV-DO network if LTE service is not available. If you choose another option and the selected network is not available, the device will not be able to connect to the cellular network. For example, if you select LTE Only and you are in an area where there is no LTE network available, the device will not be able to connect to a cellular network until you change this setting.*
Keep Alive (See Keepalive on page 116.)	
Advanced	
CDMA Mobile IP	Options are: • MIP Preferred (default) • Disabled, SIP Only • MIP Only
Network Roaming Preference	Automatic option allows home or home preferred network preference. Options are: • Automatic (default) • Home Only
Response to Incoming Ping	When a ping is received by the device from a remote location, the Response to Incoming Ping redirects it to the selected location. • No response: the incoming ping is completely ignored • ALEOS Responds (default): ALEOS returns to the Ping response. • Pass to Host: The ping is forwarded to the DMZ host with any response from the host forwarded back to the OTA location. If no host is connected, there is no ping response. *Note: Some Mobile Network Operators may block all ICMP traffic on their network. A ping sent to the device from a remote location is not received.*
LTE Authentication Mode	Specifies the authentication method to be used in the network PPP session. Options are: • NONE (default) • PAP • CHAP
Network User ID	Network User ID The login that is used to login to the cellular network, when required. • uid=user id (up to 64 bytes)

Command	Description
Network Password	Network Password is the password that, when required, is used to login to the cellular network. pw=password (30 characters maximum).
Network Watchdog (minutes)	Network connection watchdog If there is no network connection for the number of minutes configured in this field, the device reboots. This feature cannot be disabled. • 5–255 minutes (allowed values) • 120 minutes (default)

LTE—Fallback to HSPA+

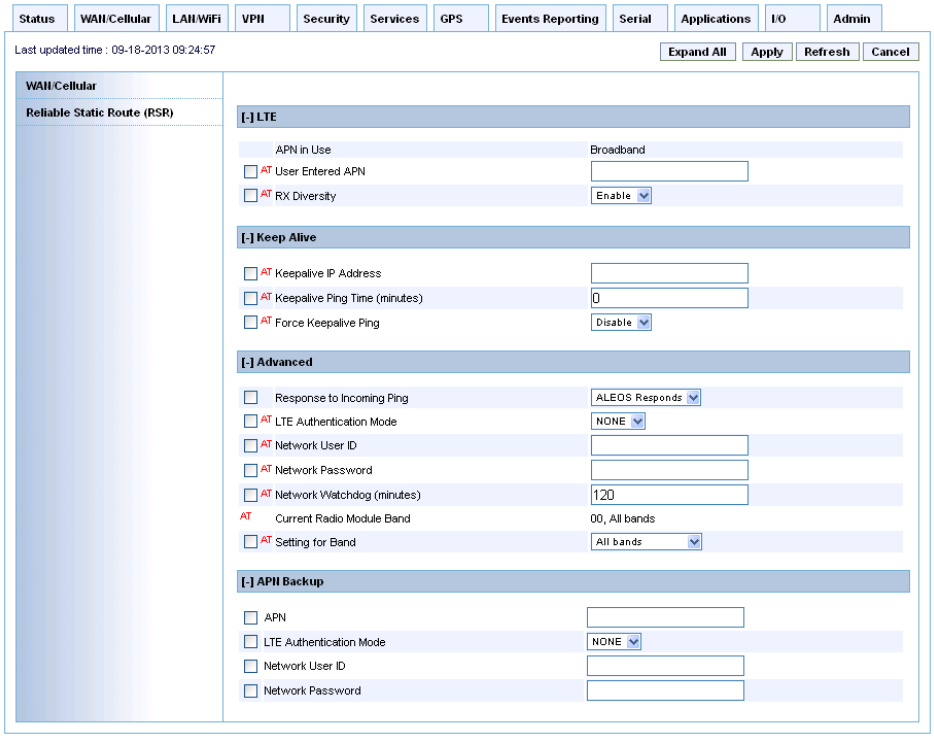
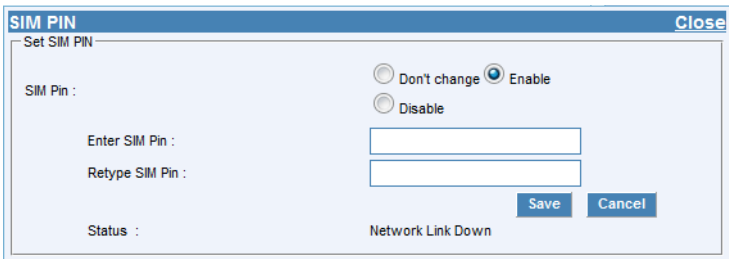


Figure 5-5: ACEmanager: WAN/Cellular—LTE - Fallback to HSPA+

Command	Description
LTE (Falls back to HSPA+)	
APN in Use	The APN in use for the current cellular connection

Command	Description
User Entered APN	Enter the desired APN. *Note: If you are activating a GX440 device using a SIM card for an account with special properties, such as a static IP APN, on the LTE network:* **1.** *Enter the static IP APN in this field.* **2.** *Click Apply.* **3.** *Click Reboot.*
RX Diversity	Allows two antennas to provide a more consistent connection • Disable • Enable (default) If you are not using a diversity antenna, diversity should be disabled. *Note: This field is not available in all AirLink devices.*
SIM PIN	If your AirLInk device has a PIN-locked SIM card installed, before the device goes on-air for the first time: **1.** Obtain the PIN from your Mobile Network Operator. **2.** Click the SIM PIN button.  **3.** Select Enable. **4.** Enter the PIN twice and click Save. *Note: On subsequent reboots and reconnects, ALEOS automatically uses the PIN. This feature prevents the SIM from being used in another device without re-entering the PIN.* *Note: You have three attempts to enter the correct PIN. If the correct PIN is not entered by the third attempt, the SIM card becomes blocked and you need a PUK code from your Mobile Network Operator to unlock it. For more information, see SIM Card is Blocked on page 397.*
Keep Alive (See Keepalive on page 116.)	
Advanced	

Command	Description
Response to Incoming Ping	When a ping is received by the device from a remote location, the Response to Incoming Ping redirects it to the selected location. • No response: the incoming ping is completely ignored • ALEOS Responds (default): ALEOS returns to the Ping response. • Pass to Host: The ping is forwarded to the DMZ host with any response from the host forwarded back to the OTA location. If no host is connected, there is no ping response. *Note: Some Mobile Network Operators may block all ICMP traffic on their network. A ping sent to the device from a remote location is not received.*
LTE Authentication Mode	Specifies the authentication method to be used in the network PPP session. Options are: • NONE (default) • PAP • CHAP
Network User ID	Network User ID The login that is used to login to the cellular network, when required. uid=user id (up to 64 bytes)
Network Password	Network Password is the password that, when required, is used to login to the cellular network. pw=password (30 characters maximum).
Network Watchdog (minutes)	Network connection watchdog If there is no network connection for the number of minutes configured in this field, the device reboots. This feature cannot be disabled. • 5–255 minutes (allowed values) 120 minutes (default)
Setting the Band	This feature enables advanced users to select the RF band range or technology the AirLink device uses. Most of the time it's best to leave this field at the default setting (All bands) but there may be times when you want to select a band range or technology that you know is more stable in the region where the AirLink device is located. The list of options displayed depends on the radio module in your device and its configuration. Possible options include: • All bands (default) • Europe 3G • North America 3G • Europe 2G • GSM ALL • Europe • North America • WCDMA ALL • LTE ALL
APN Backup (See Backup APN on page 119.)	

Keepalive

Keepalive is used to test the connection to the cellular network by pinging an IP address after a specified period of inactivity. Keepalive is only recommended for users who have a remote terminated device that infrequently communicates to the network or if you have experienced issues over time where the device can no longer be reached remotely.

When Keepalive pings the IP address, an acknowledgment indicates there is an active connection to the network. If the AirLink device does not receive a response from the IP address, it makes additional attempts according to a back-off algorithm before determining the Internet connection is not functioning properly. If it determines the connection is not functioning, the device then attempts to reconnect to the Mobile Network Operator to reestablish IP connectivity.

Data Usage Using Keepalive

Keepalive is an optional feature. If you frequently pass data with your device, you most likely do not need to have Keepalive enabled. When using Keepalive, be aware that a ping moves approximately 66 bytes of data over the network and is billable by the Mobile Network Operator. The following *IPPING settings incur approximate monthly data usage in addition to any other data usage.

Command	Description
Keep Alive	
Keepalive IP Address	The IP address that the AirLink Device pings to determine if there is Internet connectivity and make sure this IP address is accessible. Set the IP address or valid Internet domain name for the AirLink device to ping to keep itself alive (online). *IPPING must to be set to a value other than 0 to enable pinging. • d.d.d.d=IP address • name=domain name *IPPINGADDR sets the IP address you want to use for the connection test. If *IPPINGADDR is left blank or is set to an invalid IP address (e.g., an IP which is unreachable or one which is not a valid IP address), device performance is adversely affected.

Command	Description
Keepalive Ping Time (minutes)	The amount of time between pings when the device is idle. Set the period to ping (if no valid packets have been received) a specified address (*IPPINGADDR) to keep the device alive (online). • Disable pinging (default) • 5-255 minutes *IPPING sets the interval, in minutes, at which you want Keepalive to test the network connection. To disable Keepalive, set *IPPING to 0 (default setting). *Note: Pings count toward your Data Usage; the more frequently pings occur, the more your Data Usage is affected. See Data Usage Using Keepalive.*
Force Keepalive Ping	Determines if the ping should occur even if the device is not idle. Forces the IP ping even if IP traffic has occurred during the time interval. • Disable (default) • Enable

Re-Activation

The Re-Activation section of the WAN/Cellular tab only appears for EV-DO/1X devices. The Re-Activation feature can only be used when a particular device that has already been activated needs re-activation. If your device needs to be reactivated, click the button labeled “Re-Activate Cellular Account”. When you click this button, the status shows the progress of the re-activation.

Note: If the provision fails, an error message appears.

After the provision process finishes, the system then restarts, as a reset is necessary to initiate the new account information.

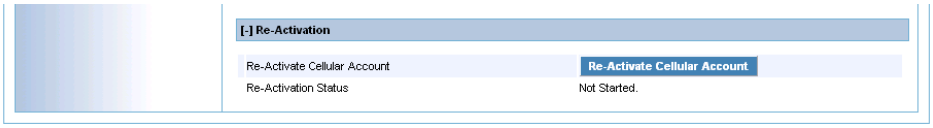


Figure 5-6: ACEmanager: WAN/Cellular > Re-Activation

Backup APN

This feature enables you to configure a backup APN to be used as a backup network connection mechanism, only if the primary APN is not available. When it is enabled, the device connects to the backup APN only if it is unable to connect to the primary APN.

Note: Switching to the backup APN can take five minutes or more, depending on the device. If the device is always connecting to the backup APN, check the primary APN to ensure that it is configured correctly.

To configure a backup APN:

1. Go to WAN/Cellular > APN Backup.

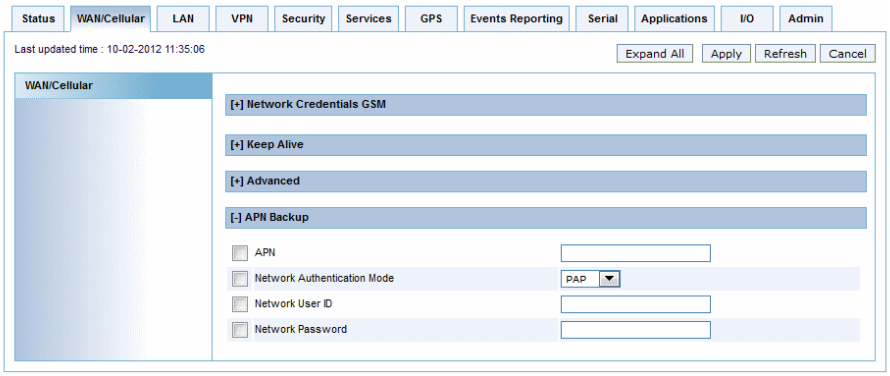


Figure 5-7: ACEmanager: WAN/Cellular > APN Backup

2. Enter the backup APN.
3. Select the Network Authentication Mode. The options are:
   - PAP (default)
   - CHAP
   - None
4. Enter the Network User ID and Password, if these are required for the wireless network.
5. Click Apply.

Reliable Static Routing (RSR)

Reliable Static Routing enables you to force specified traffic to use different routing rules (rather than the default, which is usually cellular) to direct specified traffic to a designated primary route. If the primary route fails, the specified traffic uses a backup route.

First, you designate specific traffic to use the primary route, based on the destination IP address and subnet mask. A configured tracking object test verifies the validity of the primary route. If the test fails, the backup route is used. The object test continues to run and as soon as the primary route is available, traffic is switched back to the primary route.

You can direct the traffic to a network (Figure 5-8) or to an individual host (Figure 5-9).

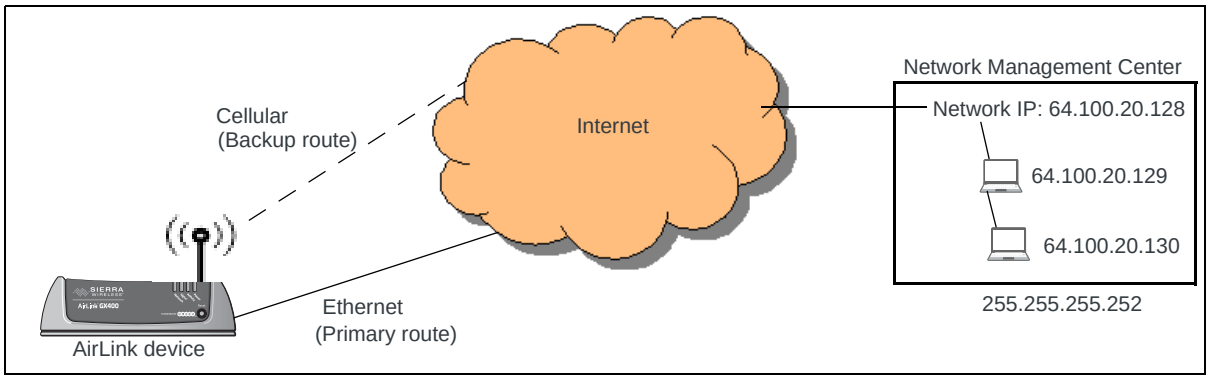


Figure 5-8: RSR directed to a destination network

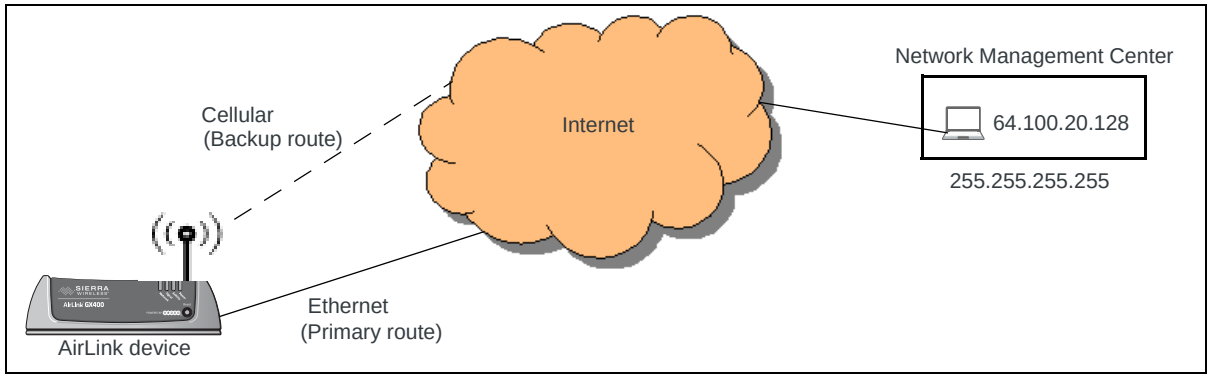


Figure 5-9: RSR directed to a destination IP address (individual host)

To configure Reliable Static Routing:

1. In ACEmanager, go to WAN/Cellular > Reliable Static Route (RSR).

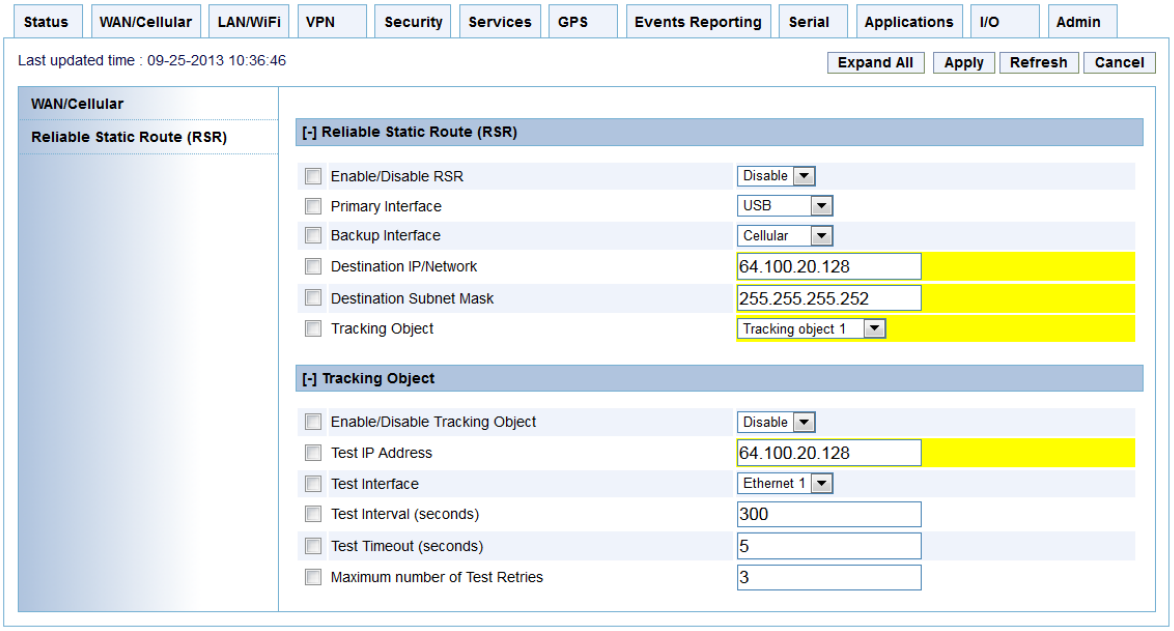


Figure 5-10: ACEmanager: WAN/Cellular > Reliable Static Route (RSR)

Note: Configure all the other fields before setting the Enable/Disable RSR field. Once you enable RSR, some fields on this page are not editable.

2. Select the interfaces for the primary and backup routes. The options are:
   - Ethernet 1 (default for primary route). If you are using a GX Series device with a Dual Ethernet X-Card installed, the additional Ethernet ports will appear in the drop-down menu as Ethernet 2 and Ethernet 3.
   - USB
   - Wi-Fi (Available only if you have a GX Series device with a Wi-Fi X-Card installed)
   - Cellular (default for backup route)
3. Set the Destination IP/Network and Destination Subnet Mask.

   To configure the RSR destination as a network, as shown in Figure 5-8, you would enter:
   - 64.100.20.128 in the Destination IP/Network field.
   - 255.255.255.252 in the Destination Subnet Mask field.

   To configure the RSR destination as an individual host, as shown in Figure 5-9, you would enter:
   - 64.100.20.128 in the Destination IP/Network field.
   - 255.255.255.255 in the Destination Subnet Mask field.
4. Set the Tracking Object (Tracking Object 1 or No Tracking Object). Normally, you would select Tracking Object 1 from the drop-down menu.
5. Under Tracking Object, leave the Enable/Disable Tracking Object set at Disable until you finish configuring the other Tracking Object fields.
6. Enter the Test IP address (normally an IP address within the Traffic Selection Criteria Network/Subnet).

7. From the drop-down menu, select the desired Test Interface (normally the same interface as the primary route). Options are:
   - Ethernet 1 (If you are using a GX Series device with a Dual Ethernet X-Card installed, the additional Ethernet ports will appear in the drop-down menu as Ethernet 2 and Ethernet 3.)
   - USB
   - Wi-Fi (Available only if you have a GX Series device with a Wi-Fi X-Card installed)
   - Cellular
8. Enter the Test Interval in seconds. This is the interval between tracking object tests.

   For most applications, the default values for the Test Interval, Test Timeout, and Maximum number of retries should be fine.

   If you want to change these values, be aware of the following:
   - Selecting a short test interval increases network traffic and may lead to false failures if the network is busy.
   - Selecting a long test interval may mean that traffic does not switch to the secondary route quickly enough when the primary route fails.
   - The test interval must be greater than the product of Test Timeout x Maximum number of Test Retries.
     [Test Interval] > [Test Timeout] x [Maximum number of Retires]
9. Enter the Test Timeout in seconds. This is the time to wait for a response. If this time expires before a response is received, the test attempt fails.
10. Enter the Maximum number of Test Retries. This is the number of times the device sends the test messages (without receiving a response) before it declares the primary network down and switches the specified traffic to the backup network.
11. In the Enable/Disable Tracking Object field, select Enable.
12. In the Enable/Disable RSR field, select Enable.

6: VPN Configuration

6

The AirLink device can act as a Virtual Private Network (VPN) device, providing enterprise VPN access to any device connected to the AirLink device even when a device has no VPN client capability on its own. The AirLink device supports three types of VPN: IPsec, GRE, and SSL. The AirLink device can support up to five VPN tunnels at the same time.

IPsec

The IP protocol that drives the Internet is inherently insecure. Internet Protocol Security (IPsec), which is a standards-based protocol, secures communications of IP packets over public networks.

IPsec is a common network layer security control and is used to create a virtual private network (VPN).

The advantages of using the IPsec feature includes:

- Data Protection: Data Content Confidentiality allows you to protect your data from any unauthorized view, because the data is encrypted (encryption algorithms are used).
- Access Control: Access Control implies a security service that prevents unauthorized use of a Security Gateway, a network behind a gateway or bandwidth on that network.
- Data Origin Authentication: Data Origin Authentication verifies the actual sender, thus eliminating the possibility of forging the actual sender's identification by a third-party.
- Data Integrity: Data Integrity Authentication allows both ends of the communication channel to confirm that the original data sent has been received as transmitted, without being tampered with in transit. This is achieved by using authentication algorithms and their outputs.

Split Tunnel

The AirLink device supports Global settings with one encrypted tunnel and one open tunnel. A sample server subnet for a Global setting would be 172.16.1.0/24. Global settings VPNs should be set up with care, as a Global settings configuration with both an enterprise VPN and access to the public Internet can inadvertently expose company resources.

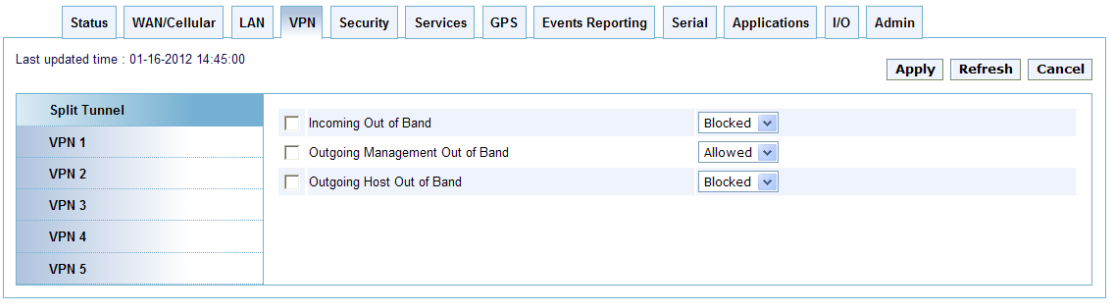


Figure 6-1: ACEmanager: VPN > Split Tunnel

Field	Description
Incoming Out of Band	Allows all incoming out of band or out of tunnel traffic Options are: Blocked (default) or Enabled
Outgoing Management Out of Band	Outgoing ALEOS out of band can be blocked or allowed (default)
Outgoing Host Out of Band	Outgoing Host out of band can be blocked (default) or allowed

VPN 1

The VPN 1 tunnel can be configured as IPsec, GRE, or SSL. Enabling any of these tunnels will expose other options for configuring the tunnel.

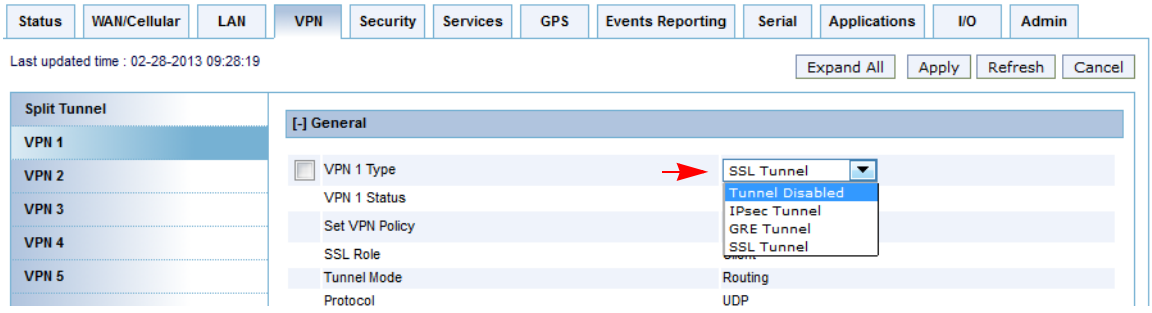


Figure 6-2: ACEmanager: VPN > VPN 1

IPsec

The IPsec architecture model includes the Sierra Wireless AirLink gateway as a remote gateway at one end communicating, through a VPN tunnel, with a VPN gateway at the other end. The remote gateway is connected to a Remote network and the VPN is connected to the Local network. The communication of data may be secured through the use of IPsec protocols.

The IPsec VPN employs the IKE (Internet Key Exchange) protocol to set up a Security Association (SA) between the AirLink device and a Cisco (or Cisco compatible) enterprise VPN server. IPsec consists of two phases to set up an SA between peer VPNs. Phase 1 creates a secure channel between the AirLink Device VPN and the enterprise VPN, thereby enabling IKE exchanges. Phase 2 sets up the IPsec SA that is used to securely transmit enterprise data.

You can specify either or both peers—local (My Identity Type field) and remote (Peer Identity Type field) using an FQDN (Fully Qualified Domain Name) or the IP address.

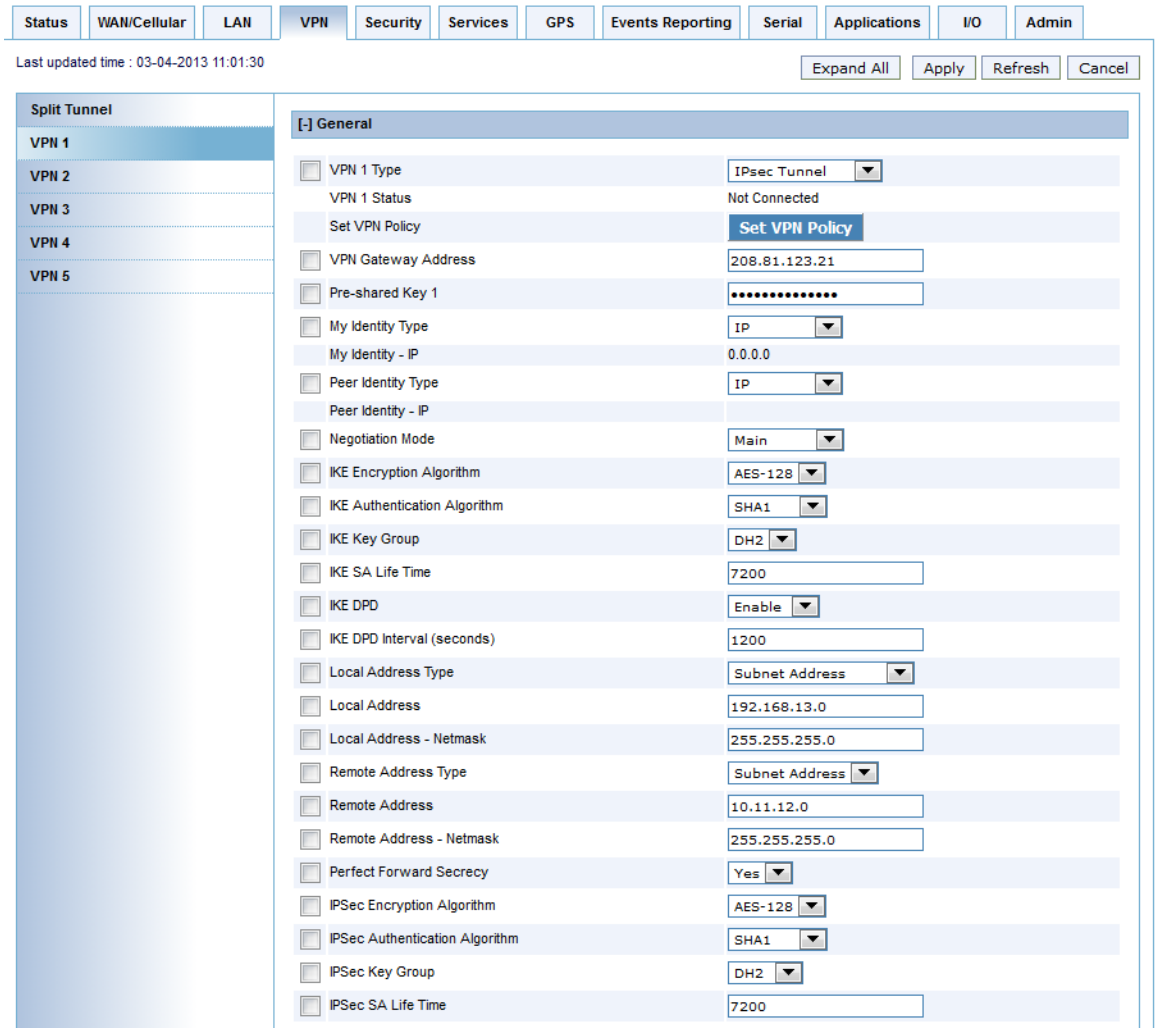


Figure 6-3: ACEmanager: VPN > VPN 1> IPsec Tunnel

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>VPN # Type</td><td>Use this field to enable or disable the VPN # tunnel. If custom settings are used, they will be saved and the tunnel can be disabled and re-enabled without needing to reenter any of the settings. For a successful configuration, all settings for the VPN tunnel must be identical between the AirLink Device VPN and the enterprise VPN server.
Options are:
• Tunnel Disabled (default)
• IPsec Tunnel
• GRE Tunnel
• SSL Tunnel</td></tr>
<tr><td>VPN # Status</td><td>Indicates the current status of the VPN # connection. Use this when troubleshooting a VPN # connection. Options are: Disabled, Not Connected, or Connected.</td></tr>
<tr><td>Set VPN Policy</td><td>Click this button to apply the new settings. The device does not need to be rebooted.</td></tr>
<tr><td>VPN Gateway Address</td><td>The IP address of the server that this VPN client connects to. This IP address must be open to connections from the AirLink device. The default VPN Gateway IP Addresses are static address on Sierra Wireless Servers. They are:
<table><tr><th>VPN</th><th>Gateway IP address</th></tr><tr><td>1</td><td>208.81.123.21</td></tr><tr><td>2</td><td>208.81.123.22</td></tr><tr><td>3</td><td>208.81.123.26</td></tr><tr><td>4</td><td>208.81.123.23</td></tr><tr><td>5</td><td>208.81.123.24</td></tr></table>You can use these default IP addresses to confirm that an IPSec connection can be established with your wireless configuration before making any configuration changes, and as an example to model your VPN configuration after. (See Figure 6-3.)</td></tr>
<tr><td>Pre-shared Key 1</td><td>Pre-shared Key (PSK) used to initiate the VPN tunnel</td></tr>
<tr><td>My Identity Type</td><td>Options are:
• IP (default) — The My Identity - IP field appears with the WAN IP address assigned by the carrier
• FQDN — The My Identity - FQDN field appears. Enter a fully qualified domain name (FQDN) e. g., modemname.domainname.com
• User FQDN — The My Identity - FQDN field appears. Enter a User FQDN whose values should include a username (e.g. user@domain.com)</td></tr>
</table>

Field	Description
My Identity - IP or **My Identity - FQDN**	• My Identity - IP appears only when IP is selected from the My Identity Type drop-down menu. The WAN IP address assigned by the carrier appears. • My Identity - FQDN appears only when User FQDN or FQDN is selected from the My Identity Type drop-down menu. Enter an FQDN or User FQDN. *Note: If you are using a FQDN for your device (My Identity) either:* • *Set up a Dynamic DNS on the Services > Dynamic DNS tab. (See Dynamic DNS on page 151.) or* • *Use a DNS server as your domain host*
Peer Identity Type	Required in some configurations to identify the client or peer side of a VPN connection. Options are: • IP (default) — The Peer Identity - IP field appears with the IP address of a VPN server set up by Sierra Wireless for your testing purposes • FQDN — The Peer Identity - FQDN field appears. Enter an FQDN (e. g. modemname.domainname.com) • User FQDN — The Peer Identity - FQDN field appears. Enter a User FQDN whose values should include a username (e.g., user@domain.com)
Peer Identity - IP or **Peer Identity - FQDN**	• Peer Identity - IP appears only when IP is selected from the Peer Identity Type drop-down menu. The VPN Gateway IP Address appears. • Peer Identity - FQDN appears only when User FQDN or FQDN is selected from the Peer Identity Type drop-down menu. Enter the Peer FQDN or Peer User FQDN.
Negotiation Mode	Enable this configuration to operate the onboard VPN under Aggressive mode. Aggressive mode offers increased performance at the expense of security. Options are: • Main (default) • Aggressive
IKE Encryption Algorithm	Determines the type and length of encryption key used to encrypt/decrypt ESP (Encapsulating Security Payload) packets. 3DES supports 168-bit encryption. AES (Advanced Encryption Standard) supports both 128-bit and 256-bit encryption. Options are: DES, 3DES, AES-128 (default), and AES-256
IKE Authentication Algorithm	MD5 is an algorithm that produces a 128-bit digest for authentication. SHA is a more secure algorithm that produces both 160-bit (SHA1) and 256-bit (SHA256) digests. Options are: MD5, SHA1 (default), and SHA256
IKE Key Group	Options are: DH1, DH2 (default), or DH5
IKE SA Life Time	Determines how long the VPN tunnel is active in seconds. Options are: 180 to 86400; Default: 7200
IKE DPD	Enable (or disable) Dead Peer Detection (DPD) When DPD is enabled, the AirLink device checks the server if there has been no traffic for a configured interval. If it does not receive an acknowledgment, it retries at 5 second intervals. If there is no acknowledgment after 5 retries, the status of the VPN is set to Not Connected and the device attempts to renegotiate IPSEC security parameters with its peer. Default is Disabled.

Field	Description
IKE DPD Interval (seconds)	Use this field to set the DPD interval (in seconds). If there has been no traffic for the period of time set in this field, the AirLink device retries checking with the server, as described in IKE DPD. Options are: 0 to 3600 (default is 1200) If this field is set to 0, DPD monitoring is turned off (or disabled as described in the IKE DPD section), but the AirLink device still responds to DPD requests from the server.
Local Address Type	The network information of the device. Options are: Use the Host Subnet, Single Address, and Subnet Address (default)
Local Address	Device subnet address
Local Address - Netmask	Device subnet mask information; 24-bit netmask Default: 255.255.255.0
Remote Address Type	The network information of the IPsec server behind the IPsec gateway. Options are: Subnet Address (default) and Single Address
Remote Address	The IP address of the device behind the gateway
Remote Address - Netmask	Remote subnet mask information. 24-bit netmask Default: 255.255.255.0
Perfect Forward Secrecy	Provides additional security through a DH shared secret value. When this feature is enabled, one key cannot be derived from another. This ensures previous and subsequent encryption keys are secure even if one key is compromised. Options are: Yes (default) or No.
IPsec Encryption Algorithm	Determines the type and length of encryption key used to encrypt/decrypt ESP (Encapsulating Security Payload) packets. 3DES supports 168-bit encryption. AES (Advanced Encryption Standard) supports both 128-bit and 256-bit encryption. Options are: None, DES, 3DES, AES-128 (default), and AES-256.
IPsec Authentication Algorithm	Can be configured with MD5 or SHA1. MD5 is an algorithm that produces a 128-bit digest for authentication. SHA is a more secure algorithm that produces both 160-bit (SHA1) and 256-bit (SHA256) digests. Options are: None, MD5, SHA1 (default), and SHA 256.
IPsec Key Group	Determines how the AirLink Device VPN creates an SA with the VPN server. The DH (Diffie-Hellman) key exchange protocol establishes pre-shared keys during the phase 1 authentication. The AirLink Device supports three prime key lengths, including Group 1 (768 bits), Group 2 (1,024 bits), and Group 5 (1,536 bits). Options are: None, DH1, DH2 (default), or DH5.
IPsec SA Life Time	Determines how long the VPN tunnel is active in seconds Options are: 180 to 86400; Default: 7200

GRE

The AirLink Device can act as a Generic Routing Encapsulation (GRE) endpoint, providing a means to encapsulate a wide variety of network layer packets inside IP tunneling packets. With this feature you can reconfigure IP architectures without worrying about connectivity. GRE creates a point-to-point link between routers on an IP network.

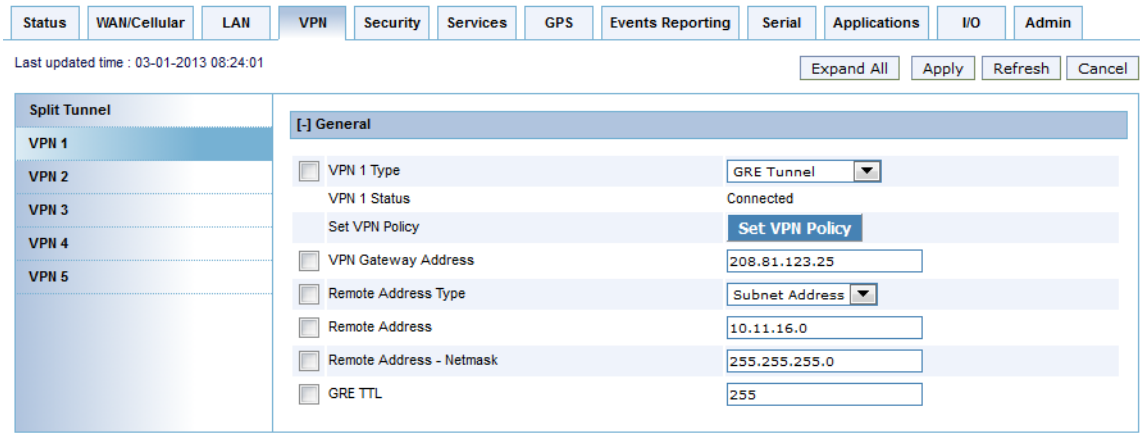


Figure 6-4: ACEmanager: VPN > VPN1 > GRE Tunnel

See the IPsec table for parameter descriptions.

Field	Description
VPN # Type	Options are: Tunnel Disabled or GRE Tunnel. Enabling the GRE Tunnel will expose other options for configuring the tunnel.
VPN # Status	Indicates the status of the GRE tunnel on the device Options are: Disabled, Connected or Not Connected
Set VPN Policy	Click this button to apply the new settings. The device does not need to be rebooted.
VPN Gateway Address	The IP address of the device that this client connects to. This IP address must be open to connections from the device.
Remote Address Type	The network information of the GRE server behind the GRE gateway
Remote Address	The IP address of the device behind the gateway
Remote Address - Netmask	The subnet network mask of the device behind the GRE gateway *Note: Never use a 16-bit subnet mask: GRE tunnel establishment will fail.*
GRE TTL	GRE time to live (TTL) value is the upper bound on the time that a GRE packet can exist in a network. In practice, the TTL field is reduced by one on every router hop. This number is in router hops and not in seconds.

SSL Tunnel

The SSL tunnel allows the device and the server to communicate across a network securely. SSL provides endpoint authentication and secure communications over the Internet.

If the SSL tunnel is selected, you can opt to secure remote communications via SSL.

The AirLink device client will authenticate the server using a PKI certificate. The server will authenticate the client via username and password. The Root CA certificate for the server certificate must be loaded on the device.

Note: SSL tunnel is based on the OpenVPN open source package. AirLink devices are SSL clients and will only talk to an SSL server (also based on the OpenVPN package).

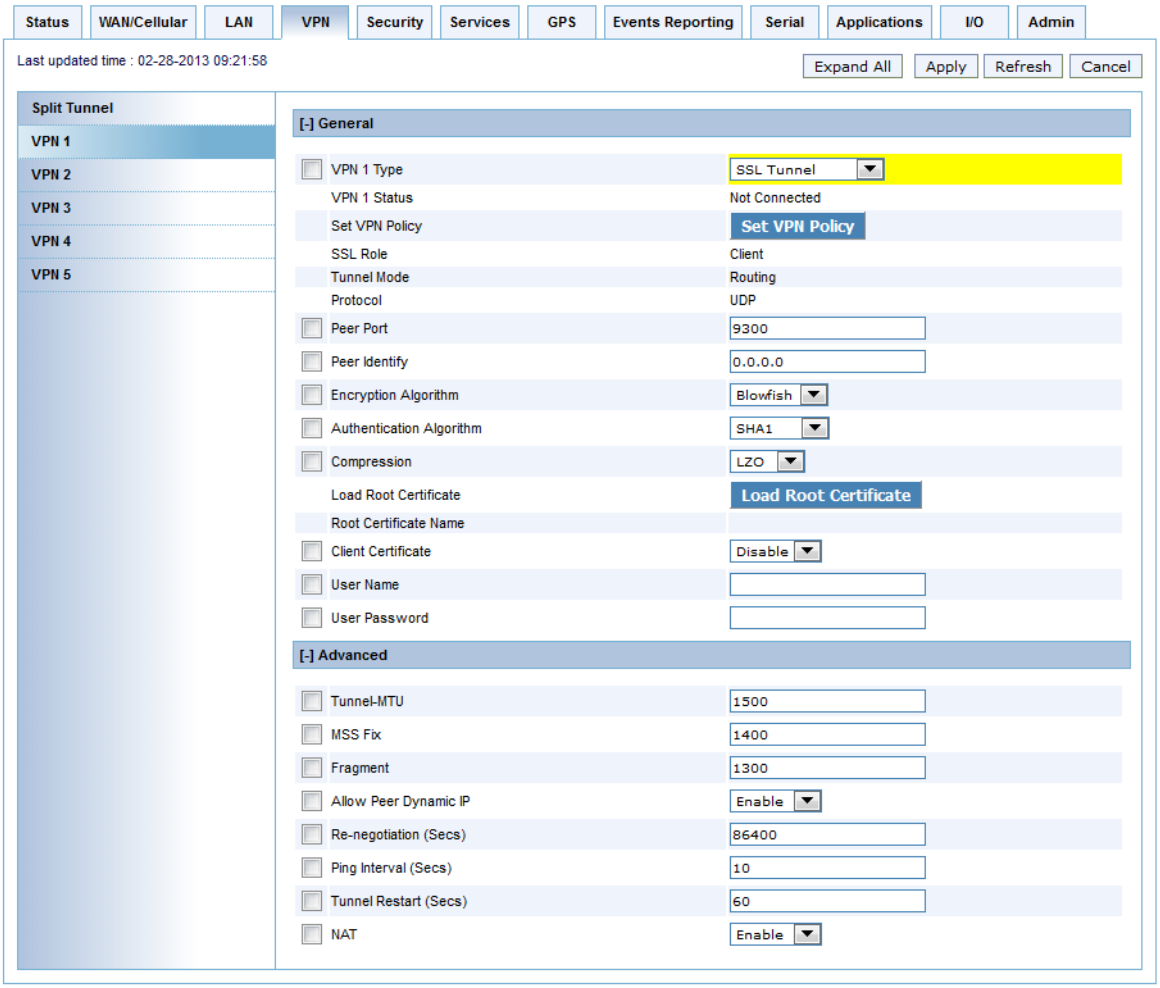


Figure 6-5: ACEmanager: VPN > VPN1 > SSL Tunnel

Field	Description
VPN 1 Type	Options are: Tunnel Disabled or SSL Tunnel. Enabling the SSL Tunnel will expose other options for configuring the tunnel.
VPN 1 Status	Indicates the status of the SSL tunnel on the device Options are: Disabled, Connected or Not Connected
Set VPN Policy	Click this button to apply the new settings. The device does not need to be rebooted.

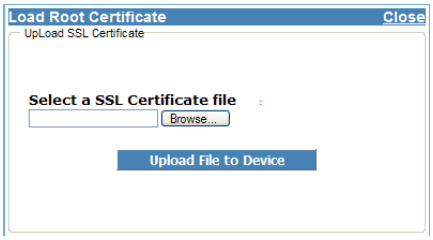
Field	Description
SSL Role	The AirLink device can only be an SSL client. Default: Client
Tunnel Mode	The Tunnel Mode is set to “Routing”.
Protocol	Displays the protocol used for configuration. Only supports UDP
Peer Port	The Peer Port is the UPD port on the peer device.
Peer Identity	Enter the IP address or Fully Qualified Domain Name (FQDN) of the peer device.
Encryption Algorithm	Options are: DES, Blowfish, DES, Cast128, AES-128, and AES-256
Authentication Algorithm	Options are: MD5, SHA-1, and SHA-256
Compression	Options are: LZ0 or NONE
Load Root Certificate	Load Root Certificate loads the server root CA certificate. When the button is selected, a window pop-ups and enable you to browse and select the file containing the root CA certificate. *Note: Although the certificate file for each device is unique to that device, they must all have the file name, home.crt. If you have multiple devices, be sure to organize the certificate files so you can distinguish which file is for which device.*
Root Certificate Name	The Root Certificate Name will display here
User Name	The user name required for client authentication
User Password	The user password required for client authentication
Tunnel-MTU	Default: 1500 bytes
MSS Fix	Default: 1400 bytes
Fragment	Default: 1300 bytes
Allow Peer Dynamic IP	Options are: Enable or Disable
Re-negotiation (seconds)	Default: 24 hours
Ping Interval (seconds)	This is the keep-alive sent by the client. Default: 0 seconds
Tunnel Restart (seconds)	Enter the time for a tunnel restart (unit in seconds)
NAT	Options are: Enable or Disable. Note that this is a Carrier NAT, not a local NAT

Load Root Certificate

Once you accept the default certificate, the SSL connection can be completed.

To load a root certificate,

1. Click Load Root Certificate.
   The following dialog-box appears.



2. Select the SSL Certificate File for your device.
3. Click Upload File to Device.

VPN 2 to VPN 5

The VPN 2 through VPN 5 sections only allow configuration of the IPsec and GRE tunnels on the device. Figure 6-3 shows the screen display for the VPN 2 submenu; screen data fields for the VPN 3, 4, and 5 submenus are identical.

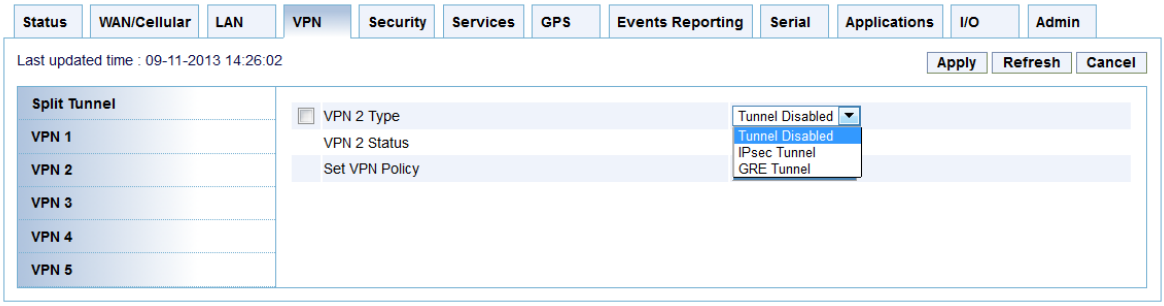


Figure 6-6: ACEmanager: VPN > VPN 2

There are three options in the scroll down menu: Tunnel Disabled, IPsec Tunnel, and GRE Tunnel. Enabling the IPsec or GRE Tunnel will expose other options for configuring that tunnel. The options shown in Figures 6-3 and 6-4 for VPN 1 are the same for VPNs 2 through 5.

7: Security Configuration

7

The security tab covers firewall-type functions. These functions include how data is routed or restricted from one side of the device to the other, i.e., from computers or devices connected to the device (LAN) and from computers or devices contacting it from a remote source (WAN). These features are set as rules.

Tip: *For additional security, Sierra Wireless recommends that you change the default password for ACEmanager. See* *Change Password on page 261.*

Solicited vs. Unsolicited

How the device responds to data being routed from one network connection to the other depends on the origin of the data.

- If a computer on the LAN initiates a contact to a WAN location (such as a LAN connected computer accessing an Internet web site), the response to that contact is solicited.
- If, however, a remote computer initiates the contact (such as a computer on the Internet accessing a camera connected to the device), the connection is considered unsolicited.

Port Forwarding

In Port Forwarding, any unsolicited data coming in on a defined Public Port is routed to the corresponding Private Port and Host IP of a device connected to the specified Physical Interface. You can forward a single port or a range of ports.

Note: Port Forwarding requires Private Mode. See *Private and Public Mode on page 67.*

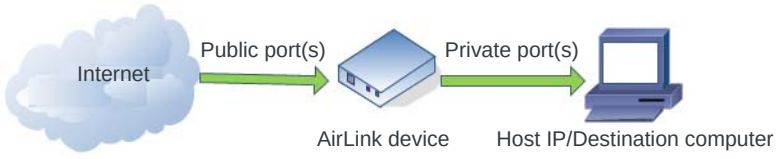


Figure 7-1: Port Forwarding

Single port

To define a port forwarding rule for a single port:

1. In ACEmanager, go to Security > Port Forwarding.

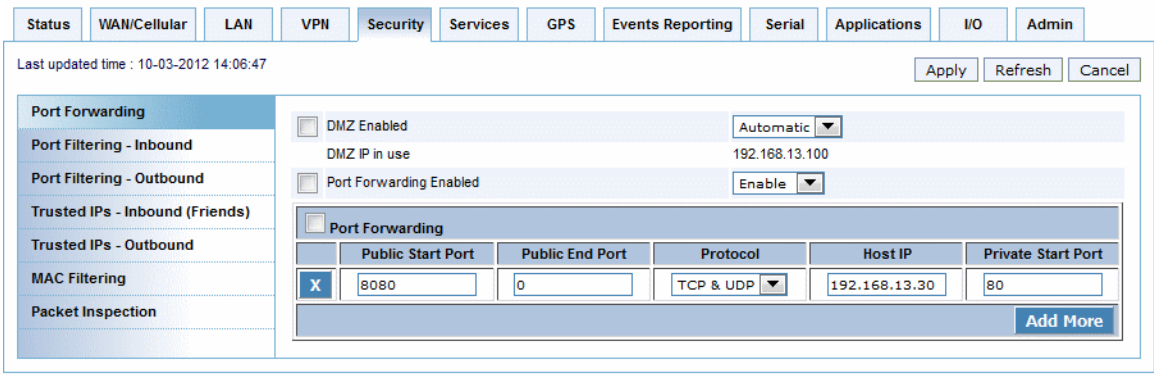


Figure 7-2: ACEmanager: Security > Port Forwarding (Single Port)

2. In the Port Forwarding Enabled field, select Enable.
3. Click “Add More” to display a rule line.
4. In the Public Start Port field, enter the desired public network port number. Values between 1 and 65535 are supported, although Sierra Wireless recommends using a value greater than 1024.

   Unsolicited data coming in on this port is forwarded to the port you select in the Private Start Port field.
5. In the Public End Port field, enter 0.
6. Select the desired protocol (see Protocol on page 136):
   - TCP
   - UDP
   - TCP & UDP
7. Enter the IP address of the computer you want to forward data to.
8. In the Private Start Port field, enter the number of the port on the destination computer that you want to forward data to.
9. Click Apply.
10. Reboot.

    You do not need to reboot immediately, if you have additional changes to make, but port forwarding does not take effect until the device is rebooted.

Range of ports

To define a port forwarding rule for a range of ports:

1. In ACEmanager, go to Security > Port Forwarding.

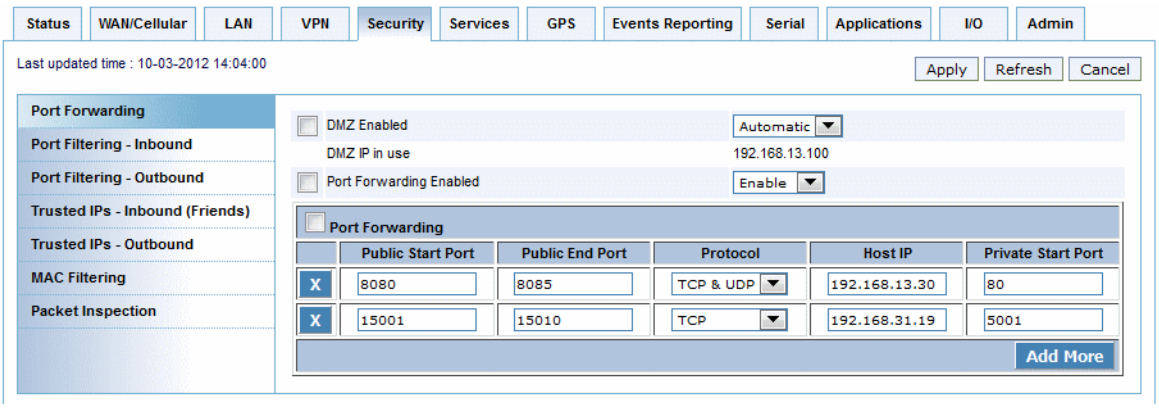


Figure 7-3: ACEmanager: Security > Port Forwarding (Port Range)

2. In the Port Forwarding Enabled field, select Enable.
3. Click “Add More” to display a rule line.
4. Set the port range for incoming data:
   a. In the Public Start Port field, enter the desired public network port number. Values between 1 and 65535 are supported, although Sierra Wireless recommends using a value greater than 1024.
   b. In the Public Port End field, enter the last public network port number in the range. The value you enter in the Public Port End field must be greater than the value in the Public Start Port field, or ALEOS rejects the selection.

      Unsolicited data coming in on ports in this range are forwarded to a range of ports, starting with the port you select in the Private Start Port field.
5. Select the desired protocol (see Protocol on page 136):
   - TCP
   - UDP
   - TCP &UDP
6. Enter the IP address of the computer you want to forward data to.
7. In the Private Start Port field, enter the starting port number for the range of ports on the destination computer that you want to forward data to.
8. Click Apply.
9. Reboot.

   You do not need to reboot immediately, if you have additional changes to make, but port forwarding does not take effect until the device is rebooted.

Note: Sierra Wireless recommends that the total number of port forwardings be fewer than 1000 ports, including single port forwarding and port forwarding within a range.

Field	Description
Port Forwarding Enabled	Enables port forwarding rules. Options are Enable and Disable (default).
Public Start Port	Port on the public network or starting port on the public network for a range of ports. • Supported values: 1–65535 (Recommended values: greater than 1024)
Public End Port	Ending port for a range of ports on the public network. • For a single port forwarding, this field must be 0. • For a range of ports, this value must be greater than the value in the Public Start Port field.
Protocol	The protocol to be used with the forwarded port: • TCP—Only those unsolicited data requests using TCP are forwarded • UDP—Only those unsolicited data requests using UDP are forwarded • TCP & UDP—Unsolicited data requests using either TCP or UDP are forwarded
Host IP	IP address of the computer (or device) you want to forward data to.
Private Start Port	Port on the destination computer used as the port for single port forwarding rules, or as the start port for a port forwarding range.

Port Forwarding Example

The following example shows you how to configure a port forward rule for a range of 6 ports on an Ethernet-connected device:

1. In ACEmanager, go to Security > Port Forwarding, and enable Port Forwarding.
2. Click “Add More” to display a rule line.
3. Enter 8080 for the Public Start Port.
4. Enter 8085 for the Public End Port.
5. Select TCP & UDP.
6. Enter 192.168.13.30 as the Host IP.
7. Enter 80 as the Private Start Port.

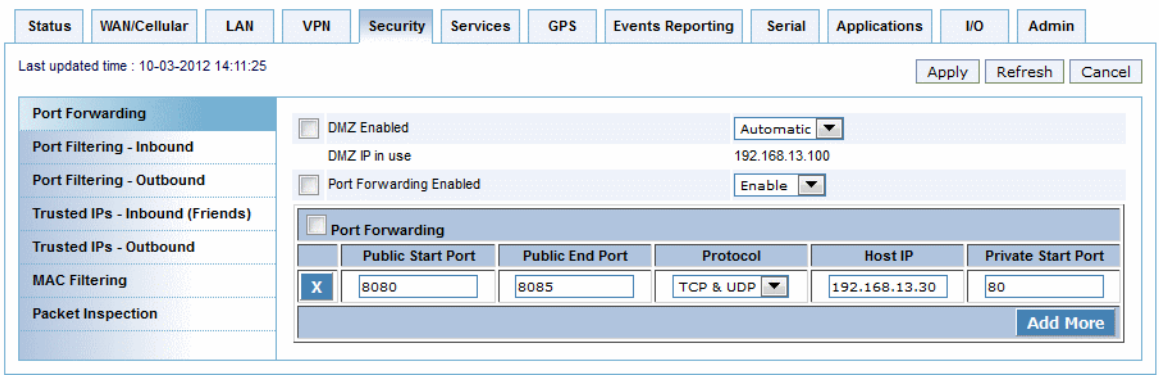


Figure 7-4: ACEmanager: Port Forwarding example

8. Click Apply.
9. Reboot.

   You do not need to reboot immediately, if you have additional changes to make, but port forwarding does not take effect until the device is rebooted.

An unsolicited TCP and UDP data request coming in to the AirLink device on port 8080 is forwarded to the LAN connected device, 192.168.13.30, at port 80. In addition, an unsolicited data request coming in from the Internet on port 8081, 8082, 8083, 8084, and 8085 is forwarded to ports 81, 82, 83, 84, and 85 respectively.

DMZ

The DMZ is used to direct unsolicited inbound traffic to a specific LAN connected host, such as a computer running a web server or other internal application. The DMZ with public mode is particularly useful for certain services like VPN, NetMeeting, and streaming video that may not work well with a NAT router.

Options for DMZ are Automatic, Manual, and Disable.

Automatic uses the first connected host. If more than one host is available (multiple Ethernet on a switch connected to the device and/or Ethernet with USBnet) and you want to specify the host to use as the DMZ, select Manual and enter the IP address of the desired host.

Note: DMZ requires Private Mode.

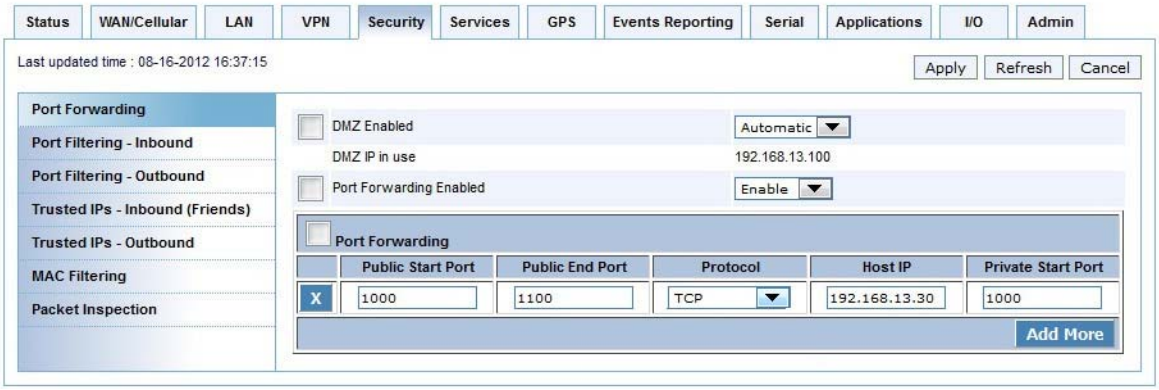


Figure 7-5: ACEmanager: Security > Port Forwarding

Field	Description
DMZ Enabled	The AirLink device allows a single client to connect to the Internet through a demilitarized zone (DMZ). Options are Automatic (default), Manual, and Disable. • Automatic—enables the first connected host or the Public Mode interface as the DMZ • Manual—inserts a specific IP address in the DMZ IP field • Disable—no connected host receives unsolicited traffic from the cellular network or Internet *Note: You can use a host connected to either Ethernet port on a Dual Ethernet X-Card as the host for Auto or Manual DMZ.*
DMZ IP	This field only appears if Manual is selected for the DMZ Enabled field; this field does not display if the DMZ is disabled. This is the IP address of the private mode host that should be used as the DMZ.
DMZ IP in use	IP address of the host to which inbound unsolicited packets are sent When the device passes the Network IP to the configured public host, the DMZ IP in Use displays the public IP.

Example of configuring the DMZ on an Ethernet connected device:

1. Enter 192.168.13.100 for the DMZ IP.
2. Select Ethernet as the Default Interface.

An unsolicited data request coming in to the AirLink device on any port is forwarded to the LAN connected device, 192.168.13.100, at the same port.

Note: The DMZ settings are independent of the number of Port Forward entries and can be used with port forwarding to pass anything not forwarded to specific ports.

Port Filtering—Inbound

Port Filtering—Inbound restricts unsolicited access to the AirLink device and all LAN-connected devices.

You can enable Port Filtering to either block or allow ports specified. When enabled, all ports not matching the rule are allowed or blocked depending on the mode.

You can configure Port Filtering either on individual ports or for a range of ports. Click Add More for each port filtering rule you want to add.

Note: Inbound restrictions do not apply to responses to outbound data requests. To restrict outbound access, you need to set the applicable outbound filter.

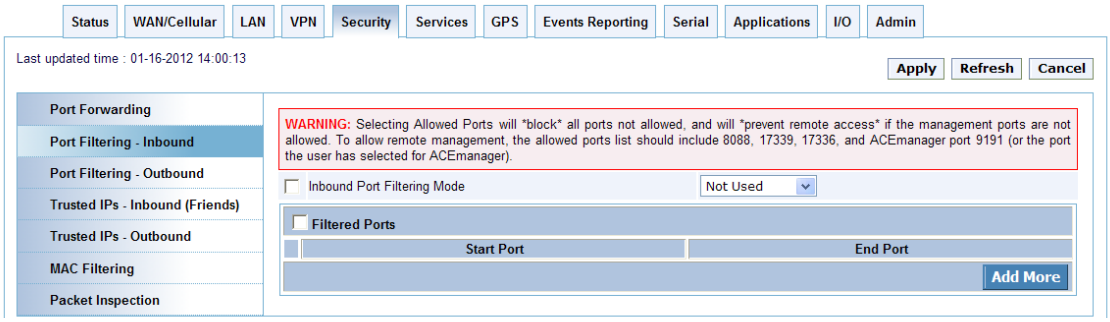


Figure 7-6: ACEmanager: Security > Port Filtering - Inbound

Field	Description
Inbound Port Filtering Mode	Options are: • Not Used (default) • Blocked Ports—ports though which traffic is blocked. Listed below. • Allowed Ports—ports through which traffic is allowed. Listed below.
Filtered Ports	
Start Port	The first of a range or a single port on the public network (cellular network accessible).
End Port	The end of the range on the public network (cellular network accessible).

Warning: *Selecting Allowed Ports will *block* all ports not allowed, and will *prevent remote access* if the management ports are not allowed. To allow remote management, the allowed ports list should include 8088, 17339, 17336, and ACEmanager port 9191 (or the port you selected for ACEmanager).*

Port Filtering — Outbound

Port Filtering—Outbound restricts LAN access to the external network, i.e., the Internet.

Port Filtering can be enabled to block ports specified or allow ports specified. When enabled, all ports not matching the rule will be allowed or blocked depending on the mode.

Port Filtering can be configured on individual ports or for a range of ports. Click Add More for each port filtering rule you want to add.

Note: Outbound restrictions do not apply to responses to inbound data requests. To restrict inbound access, you need to set the applicable inbound filter.

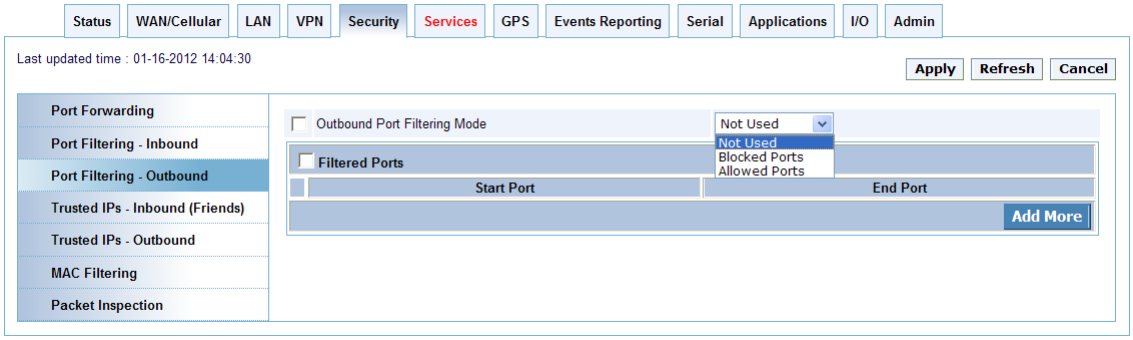


Figure 7-7: ACEmanager: Security > Port Filtering - Outbound

Field	Description
Outbound Port Filtering Mode	Allowed and blocked ports through which traffic is either allowed or blocked (respectively) are listed. Default: Not Used *Note: Outbound IP filter supports up to 9 ports.*
Start Port	The first of a range or a single port on the LAN
End Port	The end of the range on the LAN

Trusted IPs—Inbound (Friends)

Trusted IPs—Inbound restricts unsolicited access to the AirLink device and all LAN connected devices.

Tip: *Trusted IPs-Inbound was called Friends List in legacy AirLink products.*

When enabled, only packets with source IP addresses matching those in the list or range of trusted hosts will have unrestricted access to the AirLink device and/or LAN connected devices.

Note: Inbound restrictions do not apply to responses to outbound data requests. To restrict outbound access, you need to set the applicable outbound filter.

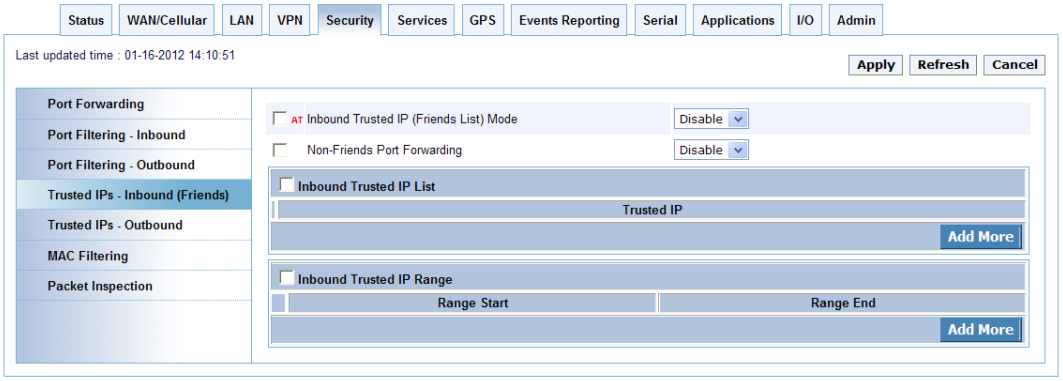


Figure 7-8: ACEmanager: Security > Trusted IPs > Inbound (Friends)

Field	Description
Inbound Trusted IP (Friend's List) Mode	Disables or Enables port forwarding rules. Options are Disable (default) or Enable.
Non-Friends Port Forwarding	Non-Friends port forwarding is like an allow rule for any of the forwarded ports. If it is enabled, the port forwarding rules apply to all incoming packets. If it is disabled, only Friends List IPs get through. Options are Disable (default) or Enable.
Trusted IP	Each entry can be configured to allow a single IP address, for example 64.100.100.2, or the IP addresses from a complete subnet, such as 64.100.10.255 allowing all IP addresses from 64.100.10.0 to 64.100.10.255.
Range Start	Specify the IP address range that is allowed access, for example 64.100.10.2 to start and 64.100.10.15 to end would allow 64.100.10.5 but would not allow 64.100.10.16.
Range End	

Trusted IPs—Outbound

Trusted IPs—Outbound restricts LAN access to the external network (Internet).

When enabled, only packets with the destination IP addresses matching those in the list of trusted hosts will be routed from the LAN to the external location.

Note: Outbound restrictions do not apply to responses to inbound data requests. To restrict inbound access, you need to set the applicable inbound filter.

Figure 7-9: ACEmanager: Security > Trusted IPs - Outbound

Field	Description
Outbound Firewall Mode	Disables or Enables port forwarding rules. Options are Disable (default) or Enable.
Outbound Trusted IP List	Each entry can be configured to allow a single IP address (e.g., 64.100.100.2) or the IP addresses from a complete subnet (e.g., 64.100.10.255) allowing all IP addresses from 64.100.10.0 to 64.100.10.255.

MAC Filtering

MAC filtering restricts LAN connection access. You can create a list of up to 20 devices that are allowed a connection based on their MAC address. When MAC filtering is enabled, devices not on the allowed list are explicitly blocked. Hosts directly connected to the device but not in the Allowed list may show an active physical connection, but are blocked from sending traffic of any kind to the device or any other host connected to the device.

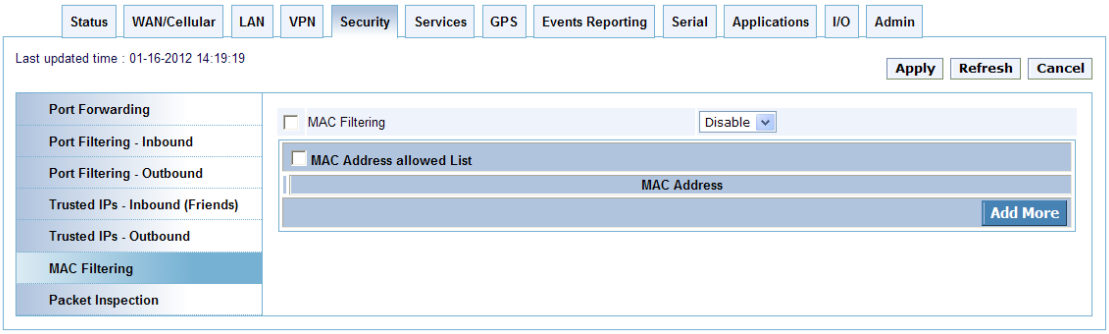


Figure 7-10: ACEmanager: Security > MAC Filtering

Field	Description
MAC Filtering	Enable or disable (default) MAC Filtering
MAC Address allowed List	Allows devices with the MAC Addresses listed to connect to the host and transfer data. Add MAC addresses by clicking on the Add More button. When adding MAC addresses, use a colon between the digit groups, for example 01:23:45:67:89:ab. *Note: After adding all the desired MAC addresses, reboot the device. The MAC Address allowed list takes effect after the device is rebooted.*
MAC Address	This is the MAC Address of the interface adapter on a computer or other device. **Tip:** *You can use the Status > LAN/WiFi page to obtain the MAC addresses of DHCP connected hosts.*

Packet Inspection

The Packet Inspection group supports two modes of security—Normal (default) and High Security. A Stateful Packet Inspection (SPI) firewall is a firewall that tracks the states of network connections and makes decisions on packet forwarding based on the states defined in the accept or reject policy rules.

Use of an SPI firewall allows for additional device security by implementing default packet state filtering policies.

Such a firewall typically passes all outgoing packets through, but only allows incoming packets if they are part of an “Established” connection, ensuring security. Stateful firewalls are able to track the state of flows in connectionless protocols (UDP) and connection oriented protocols (TCP).

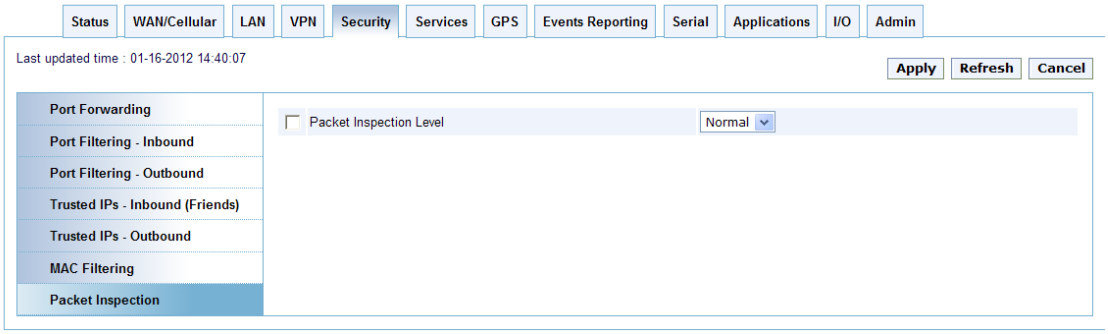


Figure 7-11: ACEmanager: Security > Packet Inspection

Field	Description
Packet Inspection Level	Enable or disable MAC Filtering Default: Normal

8: Services Configuration

The Services tab sections allow the configuration of external services that extend the functionality of the AirLink Device.

AVMS (AirVantage Management Service)

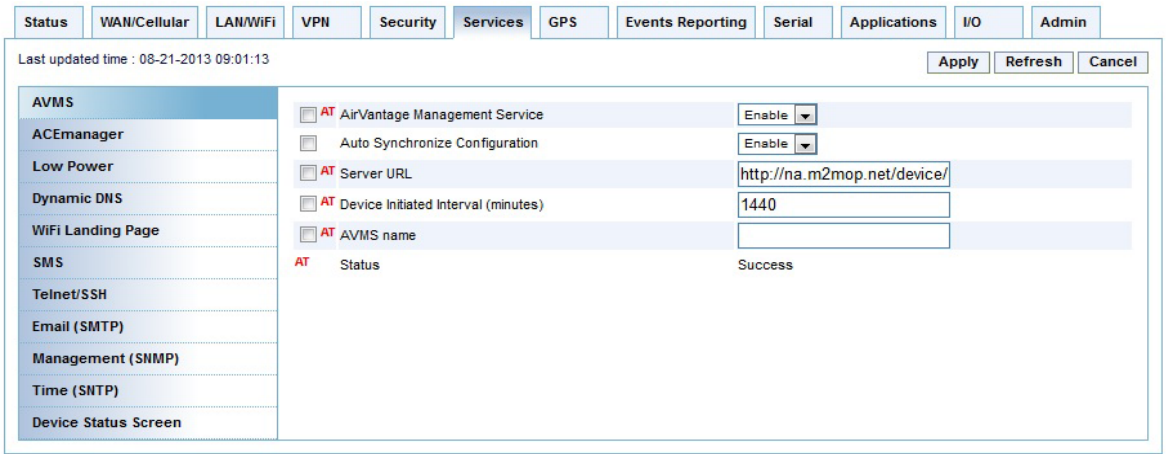


Figure 8-1: ACEmanager: Services > AVMS

Field	Description
AirVantage Management Service	Disables or enables AVMS management by disabling or enabling periodic device-initiated communication with the AVMS server.
Auto Synchronize Configuration	This field allows you to choose when changes to the configuration are propagated to AVMS. • Enable—Changes to the configuration are propagated as soon as possible and do not wait for the next communication period (as configured in the Device Initiated Interval field). This may result in more frequent communication with AVMS. (default) • Disable—Changes to the configuration are propagated to AVMS at the device initiated interval rate.
Server URL	The AVMS server URL address. By default, this is http://na.m2mop.net/device/msci/com *Note: The previously-used URL, http://na.m2mop.net/device/msci is still valid. If your AirLink devices are using that URL, there is not need to update it.*

Field	Description
Device Initiated Interval (mins)	This field determines how often the AirLink device checks for software updates and settings changes from AVMS. AVMS can also query the AirLink device at a regular interval if settings allow. Refer to AirVantage Management Service documentation for more information. Default: 15 minutes.
AVMS name	Use this field to assign a name of your choice to the AirLink device, or you can use the default name provided. You can also use an AT command to assign or query the name. See *AVMS_NAME on page 345. The default name is based on the last three digits of the device's MAC address, preceded by "ID-". For example, if the MAC address is 00:11:1a:10:6a:55, the name would be ID-106a55. (To view the entire MAC address, go to Status > About.)
Status	Displays the status of the AVMS connection: • Success—Device successfully contacted AVMS during its latest communication. • Disable—AVMS communications are disabled. (Appears when the AirVantage Management Service drop-down menu is set to Disable.) For a list of error messages, see page 395.

ACEmanager

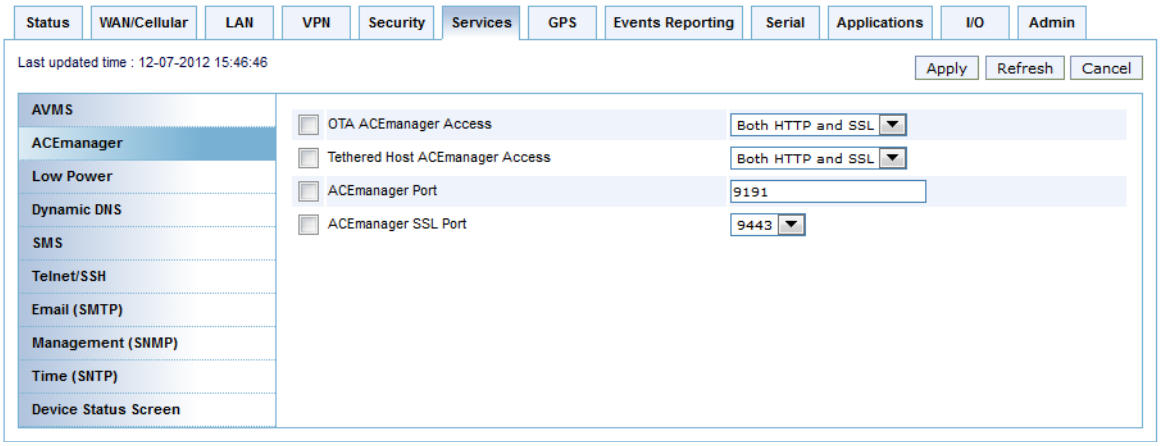


Figure 8-2: ACEmanager: Services > ACEmanager

Field	Description
OTA ACEmanager Access	Configures over-the-air ACEmanager access. Options are: • OFF • SSL Only • Both HTTP and SSL (default)
Tethered Host ACEmanager Access	Configures ACEmanager access if tethered (physically connected) to Ethernet, USB, or RS232. Options are: SSL Only and Both HTTP and SSL. (default)

Field	Description
ACEmanager Port	Identifies the port set for ACEmanager. Reboot the device after applying the port change.
ACEmanager SSL Port	Identifies the SSL port set for ACEmanager access. Reboot the device after applying the port change. Eight port Options are: • 9443 through 9449 and 443. Default: 9443

Low Power

The AirLink device switches into Low Power Mode when the ACEmanager-configured event occurs.

Low Power Mode is a standby mode whereby the AirLink processor and radio are off and a low power timer and detection circuit are operational. When ACEmanager-configured events are detected, the AirLink device powers up and automatically connects to the Mobile Network Operator's network.

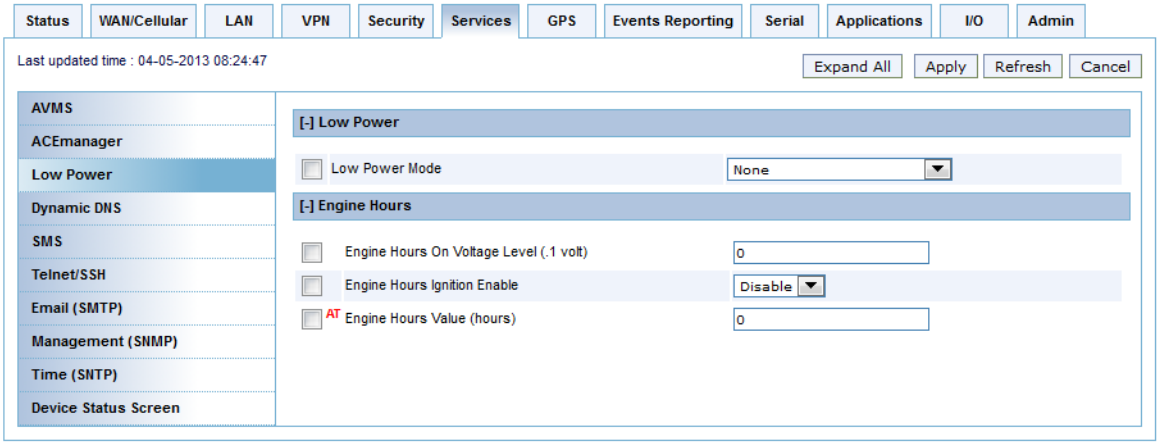
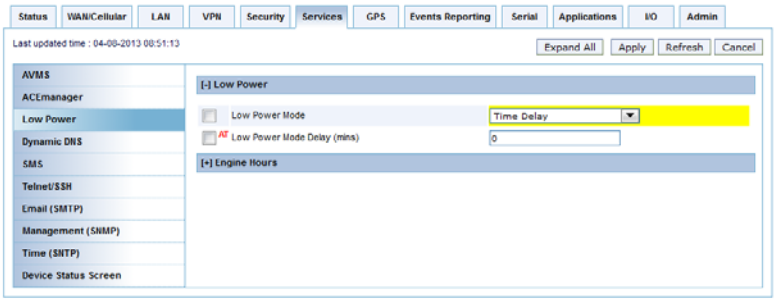
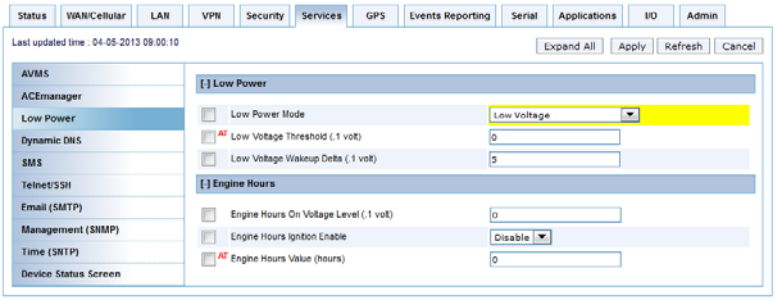
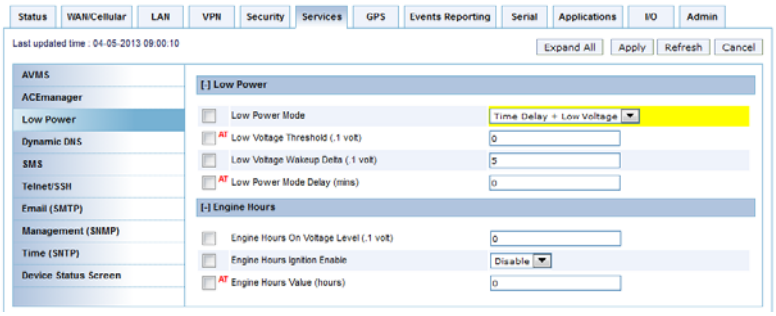
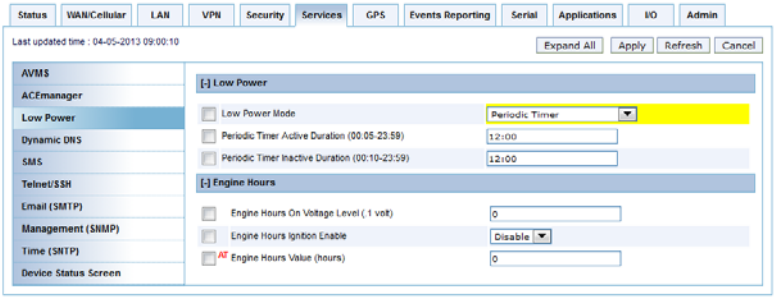
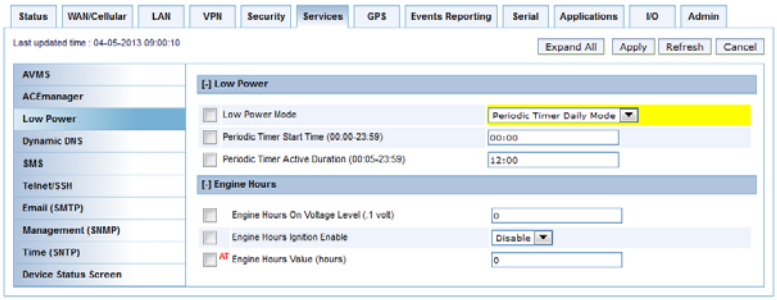


Figure 8-3: ACEmanager: Services > Low Power

Field	Description
Low Power	
Low Power Mode	Allows you to set one of the following low power mode parameters: • None (default) • Time Delay • Low Voltage • Time Delay + Low voltage • Periodic Timer • Periodic Timer Daily Mode

Field	Description
Low Power Mode (continued)	Time Delay If you select Time Delay, the AirLink device monitors the ignition sense on the power connector and enters the low power consumption stand-by mode when the ignition is turned-off.  • Low Power Mode Delay (mins): The number of minutes after one of the Low Power events happens until the AirLink device enters the low power mode. (max 255)
Low Power Mode (continued)	Low Voltage If you select Low Voltage, you need to set the Low Voltage Threshold. • Low Voltage Threshold: Set the voltage level at which the device goes into low power mode (threshold in tenths of volts), e.g. VLTG=130 would place the device in a low power standby state if the voltage goes below 13.0V. Accepted values are 80–360. • Low Voltage Wakeup Delta (.1 volt): Sets the change in voltage used to wake up the device from low power mode, e.g. set to 25 to wake up from low power mode when the input voltage exceeds the low voltage threshold by 2.5 volts. 

Field	Description
Low Power Mode (continued)	Time Delay + Low Voltage If you select this option, the device delays going into Low Power mode caused by a low voltage drop (below threshold) or ignition off.  *Note: There is always a minimum of 1 minute between the power down event and actual shutdown (to give the AirLink device time to prepare); entering zero, for Low Power Mode Delay, will not power down the device immediately.*
Low Power Mode (continued)	Periodic Timer If you select the Periodic Timer, two additional fields appear: • Periodic Timer Active Duration — Enter the time for how long the device needs to be in Active mode • Period Timer Inactive Duration — Enter the time for how long the device should be inactive after the Active mode expires. The Low Power mode process will repeat in a cyclical way (active and inactive). 

Field	Description
Low Power Mode (continued)	Periodic Timer Daily Mode This mode allows you to specify when the device should be active and when it should be in Low Power mode on a daily basis. If you select the Periodic Timer Daily Mode, two additional fields display: • Periodic Timer Start Time (00:00–23:59 UTC) — Enter the time to start the AirLink device in the Active mode. • Period Timer Active Duration (00:00–23:59 UTC) — Enter the time for how long the device should be active. The device will become active at the start time (UTC) and stay active for the active duration. 
Engine Hours — ALEOS can start and stop counting engine hours based on: • Voltage on the Power Pin from the vehicle battery (Engine Hours On Voltage Level) • Voltage on the ignition Sense Pin (Engine Hours Ignition Enable) If you configure both fields, both conditions must be met before the device begins counting engine hours.	
Engine Hours On Voltage Level (.1 Volt)	If you want to use this field to trigger counting engine hours, the AirLink device must be using the vehicle battery as a power source (i.e. Pin 1 [VCC] and Pin 2 [ground] on the AirLink device's power connector are connected to the vehicle battery).[a] Enter the voltage level above which the AirLink device starts counting engine hours. When the voltage from the vehicle battery falls below that value, the device stops counting engine hours. Enter the desired value in .1 volt units. For example, to set the voltage level at 13.0 volts, enter 130. The default value is 0, which means the feature is disabled. Engine hours are not incremented based on the power pin voltage level.

Field	Description
Engine Hours Ignition Enable	If Pin 3 (the ignition sense pin) on the AirLink device's power connector is wired to the vehicle's ignition switch[a], oil pressure switch, or some other digital input, you can use this field to trigger counting engine hours. The device starts counting engine hours when the voltage on Pin 3 is high and stops counting when the voltage is low (Ground or 0 volts). Options are: • Disable (default) Engine hours are not incremented based on changes to Pin 3. • Enable
Engine Hours Value (hours)	Displays an estimate of the number of hours the engine has been running, based on either the input voltage from the vehicle battery or the voltage on the ignition sense pin, depending on which of the two previous fields you configured. You can also set the engine hours value to an initial value. The initial default value is 0. The maximum allowed value is 65535. You can also use an AT Command to set this value. For more information, see *ENGHRS on page 345. *Note: You can configure Events Reporting to send reports based on this value. For more information, see Events Reporting Configuration on page 207.*

a. For more information, refer to the AirLink GX Series or LS300 User Guide (Power Connector Description in Chapter 2: Installation and Setup).

Dynamic DNS

Dynamic DNS allows an AirLink device WAN IP address to be published either to a proprietary Sierra Wireless dynamic DNS service called IP Manager, or to an alternate third party Mobile Network Operator.

Whether you have one Sierra Wireless AirLink device or multiple devices, it can be difficult to keep track of the current IP addresses especially if the addresses are not static but change every time the devices connect to the cellular network. If you need to connect to a specific gateway, or the device behind it, it is much easier when you have a domain name (car54.mydomain.com, where are you?).

Reasons to Contact or Connect to a Device:

- Requesting a location update from a delivery truck
- Contacting a surveillance camera to download logs or survey a specific area
- Triggering an oil derrick to begin pumping
- Sending text to be displayed by a road sign
- Updating the songs to be played on a juke box
- Updating advertisements to be displayed in a cab
- Remote accessing a computer, a PLC, an RTU, or other system
- Monitoring and troubleshooting the status of the device itself without needing to bring it in or go out to it.

A dynamic IP address is suitable for many Internet activities such as web browsing, looking up data on another computer system, for data only being sent out, or for data only being received after an initial request (also called Mobile

Originated). However, if you need to contact the AirLink device directly, a device connected to the AirLink device, or a host system using your AirLink device (also called Mobile Terminated), a dynamic IP will not give you a reliable address to contact (since it may have changed since the last time it was assigned).

Domain names are often only connected to static IP addresses because of the way most domain name (DNS) servers are set-up. Dynamic DNS servers require notification of IP Address changes so they can update their DNS records and link a dynamic IP address to the correct name.

- Dynamic IP addresses are granted only when your AirLink device is connected and can change each time the gateway reconnects to the network.
- Static IP addresses are granted the same address every time your AirLink device is connected and are not in use when your gateway is not connected.

Since many cellular providers, like wire-based ISPs, do not offer static IP addresses or static address accounts (which can cost a premium as opposed to. dynamic accounts), Sierra Wireless AirLink Solutions developed IP Manager. IP Manager works with a Dynamic DNS server to receive notification from Sierra Wireless AirLink devices to translate the dynamic IP address to a fully qualified domain name. Thus, you can contact your AirLink device directly from the Internet using a domain name.

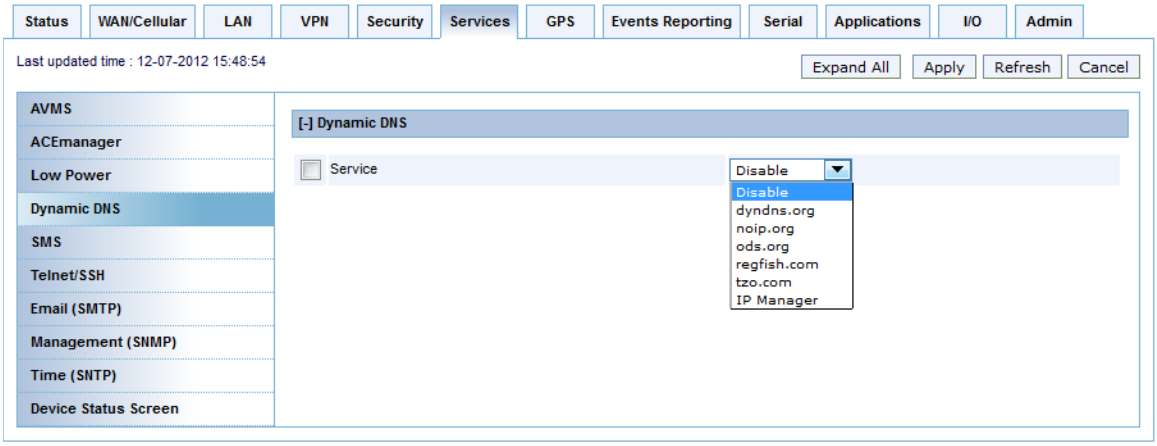


Figure 8-4: ACEmanager: Services > Dynamic DNS Service (partial screen)

Field	Description
Service	Allows you to select a Dynamic DNS Mobile Network Operator. Options are: • Disable (default) • dyndns.org • noip.org • ods.org • regfish.com • tzo.com • IP Manager

Third Party Services

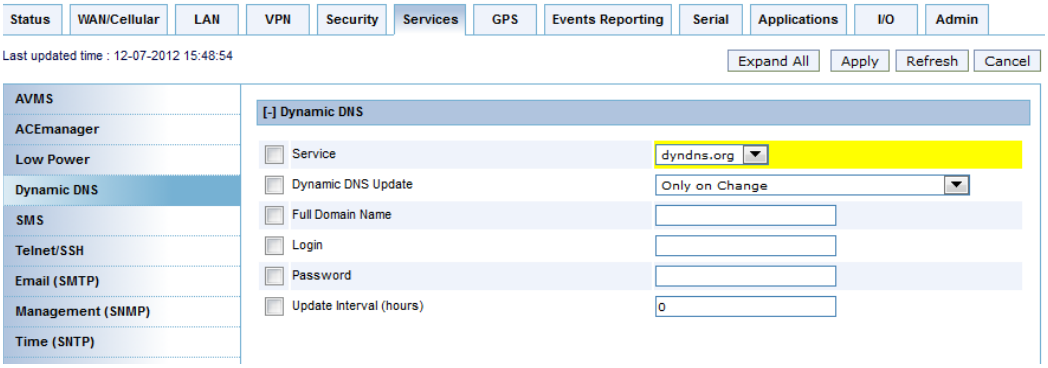


Figure 8-5: ACEmanager: Services > Dynamic DNS 3rd Party Services (partial screen)

Figure 8-5 is a sample third party service information screen. The third party service selected from the Service drop down menu in this example is "dyndns.org." These same fields will be displayed for all Service selections other than IP Manager and Disable.

Field	Description
Service	Allows you to select a Dynamic DNS Mobile Network Operator. Options are: • Disable (default) • dyndns.org • noip.org • ods.org • regfish.com • tzo.com • IP Manager
Dynamic DNS Update	Options are: • Only on Change • Periodically Update (Not Recommended)
Full Domain Name	The name of a specific AirLink gateway or device
Login	Shows the login name
Password	Shows the password in encrypted format
Update Interval (hours)	Indicates the time (in hours) between checks for service updates from the selected third party service when periodic is selected.

IP Manager

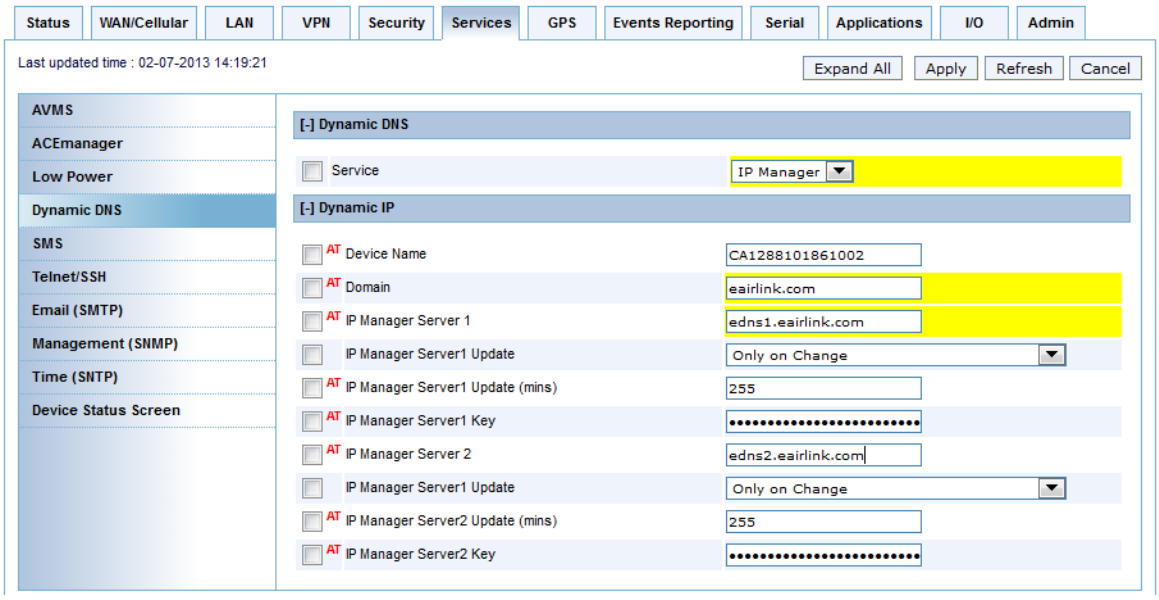


Figure 8-6: ACEmanager: Services > Dynamic DNS IP Manager

Figure 8-5 shows the Dynamic IP fields that appear after selecting IP Manager as your Dynamic DNS Service.

Field	Description
Device Name	The name you want for the device. There are some restrictions listed below for the device name.
Domain	The domain name to be used by the device. This is the domain name of the server configured for *IPMANAGER1. *Note: As a service, Sierra Wireless maintains IP Manager servers that can be used with any AirLink device. To use one of the free IP Manager servers, enter eairlink.com in this field.*
IP Manager Server 1 (IP Address) / IP Manager Server 2 (IP Address)	The IP address or domain name of the dynamic DNS server which is running IP Manager. *Note: To use the Sierra Wireless IP Manager server, enter:* *edns1.earlink.com (IP Manager Server 1)* *edns2.eairlink.com (IP Manager Server 2)*
IP Manager Server 1 Update / IP Manager Server 2 Update	Options are: • Only on Change • Periodic

Field	Description
IP Manager Server1 Update (mins) / IP Manager Server2 Update (mins)	How often, in minutes, you want the address sent to the IP Manager
IP Manager Server 1 Key / IP Manager Server 2 Key	User-defined password key used instead of the AirLink secret key when using an IP Manager server other than the one provided by Sierra Wireless.

Tip: *Some PPPoE connections can use a Service Name to differentiate PPPoE devices. Use the device name to set a Station Name for the PPPoE connection.*

Understanding Domain Names

A domain name is a name of a server or device on the Internet associated with an IP address. Similar to how the street address of your house or your phone number are ways to contact you, both the IP address and the domain name can be used to contact a server or device on the Internet. While contacting you at your house address or with your phone number employ different methods, using a domain name instead of the IP address uses the same method, just as a word based name is easier for most people to remember than a string of numbers.

Understanding the parts of a domain name can help to understand how IP Manager works and what you need to be able to configure the device. A fully qualified domain name (FQDN) generally has several parts.

- **Top Level Domain** (TLD): The TLD is the ending suffix for a domain name (.com, .net, .org, etc.)
- **Country Code Top Level Domain** (ccTLD): This suffix is often used after the TLD for most countries except the US (.ca, .uk, .au, etc.)
- **Domain name**: This is the name registered with ICANN (Internet Corporation for Assigned Names and Numbers) or the registry for a the country of the ccTLD (i.e., if a domain is part of the .ca TLD, it would be registered with the Canadian domain registry). A name must be registered before it can be used.
- **Sub-domain or server name**: A domain name can have many sub-domain or server names associated with it. Sub-domains need to be registered with the domain, but do not need to be registered with ICANN or any other registry. It is the responsibility of a domain to keep track of its own subs.

car54.mydomain.com

- ***.com*** is the TLD
- *mydomain* is the domain (usually noted as mydomain.com since the domain is specific to the TLD)
- *car54* is the subdomain or server name associated with the device, computer, or device registered with mydomain.com

car54.mydomain.com.ca

This would be the same as above, but with the addition of the country code. In this example, the country code (.ca) is for Canada.

Tip: *A URL (Universal Resource Locator) is different from a domain name in that it also provides information on the protocol used by a web browser to contact that address such as* `http://www.sierrawireless.com`. www.sierrawireless.com *is a fully qualified domain name, but http://, the protocol identifier, is what makes the whole thing a URL.*

Dynamic Names

When an IP address is not expected to change, the DNS server can indicate to all queries that the address can be cached and not looked up for a long period of time. Dynamic DNS servers, conversely, have a short caching period for the domain information to prevent other Internet sites or queries from using the old information. Since the IP address of a device with a dynamic account can change frequently, if the old information was used (e.g., with a DNS server which indicates the address can be cached for a long period of time) when the IP address changed, the domain would no longer point to the new and correct IP address of the device.

If your AirLink device is configured for Dynamic IP when it first connects to the Internet, it sends an IP change notification to the IP Manager. The IP Manager acknowledges the change and updates the Dynamic DNS server. The new IP address will then be the address for your device's configured name.

When your device IP address has been updated in IP Manager, it can be contacted by name. If the IP address is needed, use the domain name to determine the IP address.

Note: The fully qualified domain name of your AirLink device will be a subdomain of the domain used by the IP Manager server.

WiFi Landing Page

The WiFi Landing Page allows you to enable or disable the Landing Page identified by a Landing Page URL address.

This page only appears if a Wi-Fi X-Card is installed in the AirLink device.

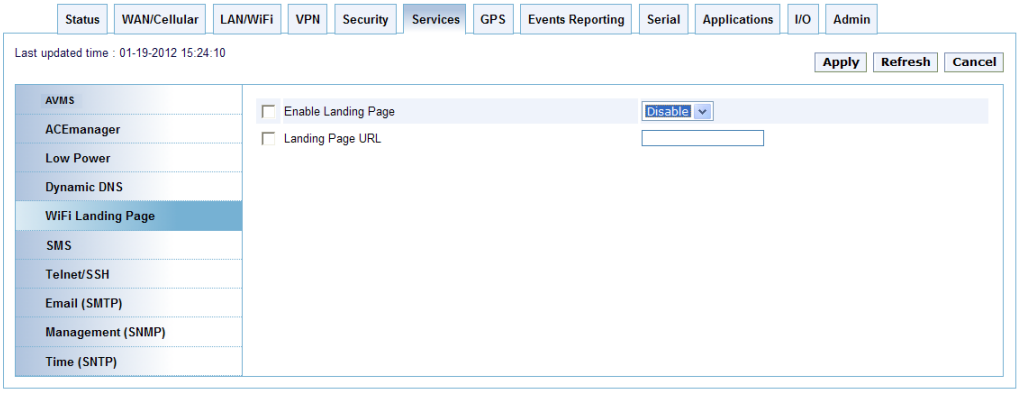


Figure 8-7: ACEmanager: Services > WiFi Landing Page

Field	Description
Enable Landing Page	Allows you to enable or disable (Default) the WiFi landing page.
Landing Page URL	A valid URL address is required to enable Internet service. This URL can include folders or subdomains (e.g., www.sierrawireless.com/airlink)

SMS

ALEOS has the ability to:

- Receive commands via SMS message and send responses
- Act as an SMS gateway for a host connected to a local interface

Note: To use SMS with your AirLink device, you must have an account with SMS enabled, and your cellular carrier cannot block SMS for data accounts.

You can choose from four SMS message modes:

- Password Only
- Control Only
- Gateway Only
- Control and Gateway

The following sections provide more information, instructions for configuring each of these modes, and sending SMS messages. For more information and a list of available commands, see page 377.

Password Only

In Password Only mode, you can send SMS commands to a device, provided you use the password.

Note: In Password Only mode, you can only send SMS commands. Non-command (gateway) SMS messaging is not supported.

Note: In Password Only mode, the password is always required. The trusted list is not used, so even if you are sending the command from a trusted number, you must include the password.

To configure Password Only mode:

1. In ACEmanager, go to Services > SMS.

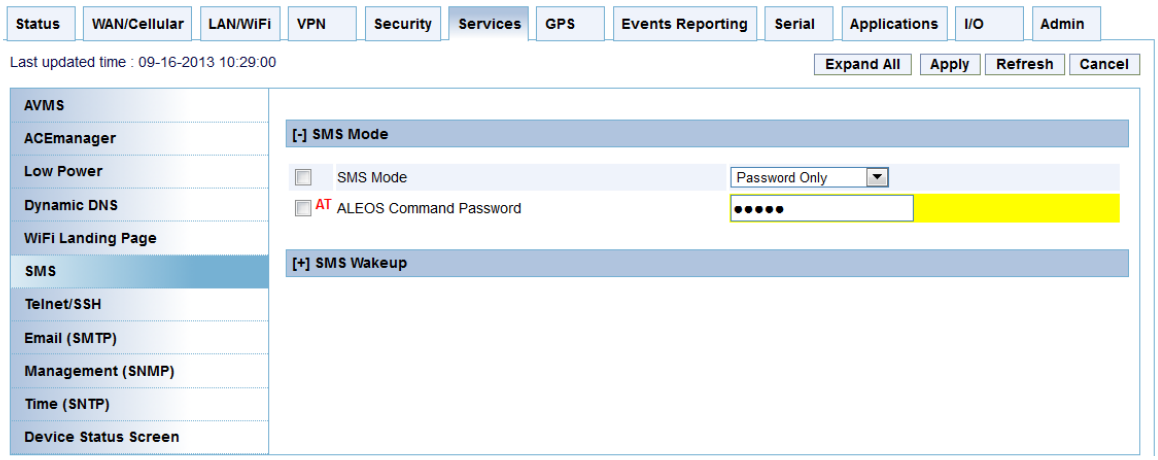


Figure 8-8: ACEmanager: Services > SMS (Password Only)

2. In the SMS Mode field, select Password Only.
3. Enter the desired password in the ALEOS Command Password field or leave the field blank to use the default password.

   The password you enter can be any alphanumeric string between 1 and 255 characters long.

   For more information see SMS Password Security on page 171.
4. Click Apply.

Sending an SMS Command

The format for sending an SMS command in Password Only mode is:
[PW] [Prefix][Command]

Example:

“PW 1234 &&&reset”, where:

- 1234 is the password (required)
  If you did not create a password when you configured SMS, use the default

password—the last 4 digits of the SIM ID number (for SIM-based devices) and the last 4 digits of the ESN (for non-SIM devices). If you do not know the SIM ID or ESN number, you can find it in ACEmanager in Status > WAN/ Cellular.

- &&& is the prefix (required)
- reset is the command

For more information on sending SMS commands and a list of available commands, see page 377.

Control Only

In Control Only mode, you can send SMS commands to a device, but you cannot send non-command (gateway) SMS messages.

If the Trusted List is enabled (see Trusted Phone Number on page 171), and your phone number is on the trusted list, you can send an SMS command without a password. If your number is not on the trusted list, you can still send an SMS command if you use the password.

Configure ALEOS for Control Only mode

1. In ACEmanager, go to Services > SMS.

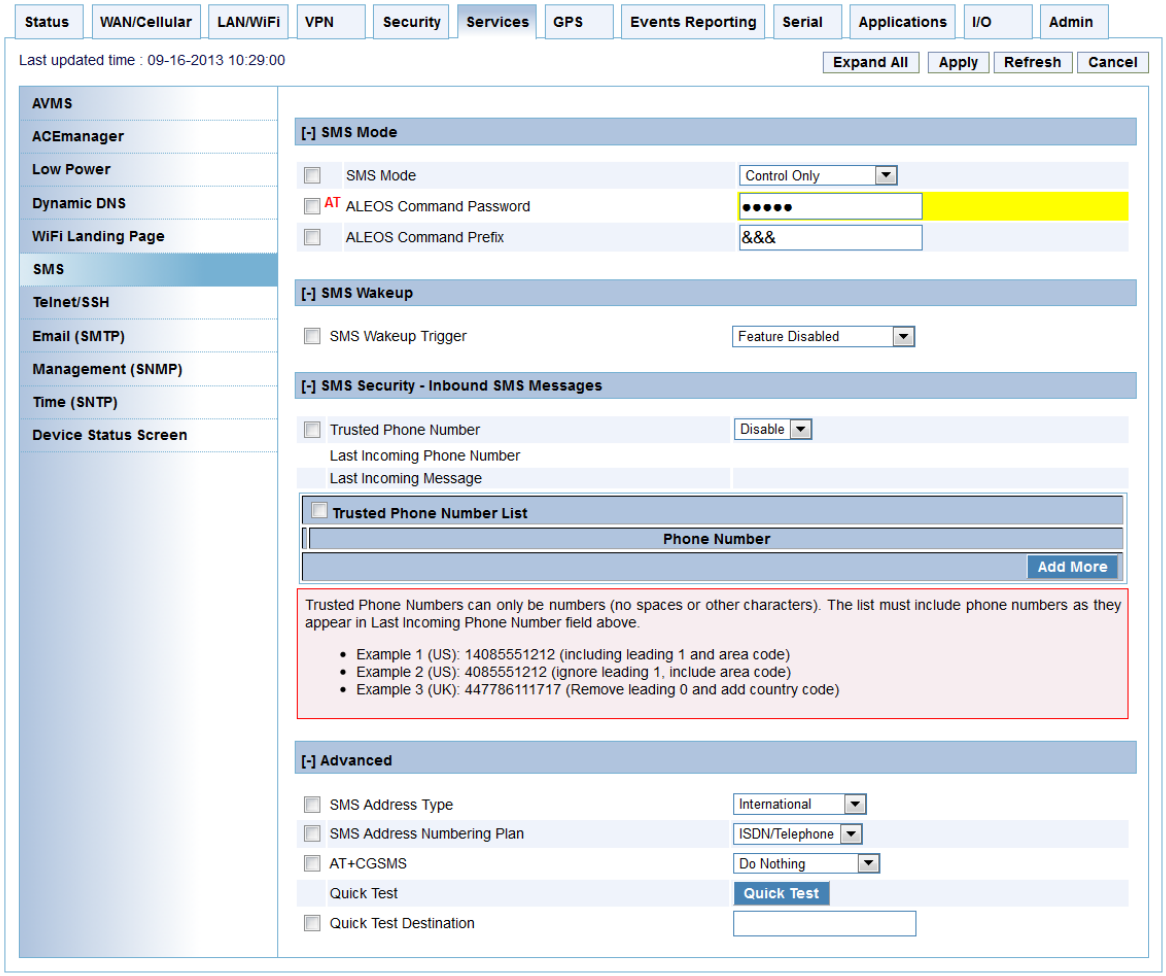


Figure 8-9: ACEmanager: Services > SMS (Control only)

2. In the SMS Mode field, select Control Only.
3. Enter the desired password in the ALEOS Command Password field or leave the field blank to use the default password.

   The password you configure can be any alphanumeric string between 1 and 255 characters long.

   For more information see SMS Password Security on page 171.

Note: If all the SMS commands you send in Control Only mode are from a trusted number, you do not need to include a password when you send the command.

4. If desired, enter the ALEOS Command Prefix or use the default prefix, &&&.

Note: If you leave the ALEOS Command Prefix field blank, no prefix is required when you send the SMS command. The option to omit the prefix is only available in Control Only mode.

5. You may also want to configure SMS Security options (see SMS Security on page 169) and Advanced options (see SMS > Advanced on page 173).
6. Click Apply.

Sending an SMS Command

The format for sending an SMS command in Control Only mode is:
[PW] [Prefix][Command]

Example:

“PW 1234 &&&reset”, where:

- 1234 is the password
  - If you are sending the SMS command from a trusted number, the password is not required. (See Trusted Phone Number on page 171.)
  - If you are sending the SMS command from a non-trusted number, the password is required.
    If you did not create a password when you configured SMS, use the default password—the last 4 digits of the SIM number (for SIM-based devices) and the last 4 digits of the ESN (for non-SIM devices). If you do not know the SIM ID or ESN number, you can find it in ACEmanager in Status > WAN/Cellular.
- &&& is the prefix
  If the ALEOS Command Prefix field in ACEmanager (Services > SMS) is blank, the prefix is not required.
- reset is the command

For information on sending SMS commands and a list of available commands, see page 377.

Gateway Only

In Gateway Only mode you can send an SMS non-command (gateway) message to a device, provided you are sending the message from a trusted number. (See Trusted Phone Number on page 171.)

SMS messages received by the device (inbound) are sent on to the configured host. Messages sent by the host to a configured port on the device are sent out as an SMS by the device (outbound). Essentially, the device forwards SMS messages between the cellular radio and the connected host.

You can also send SMS commands in Gateway Only mode, provided you use the password.

Configure ALEOS for Gateway Only mode

1. In ACEmanager, go to Services > SMS.

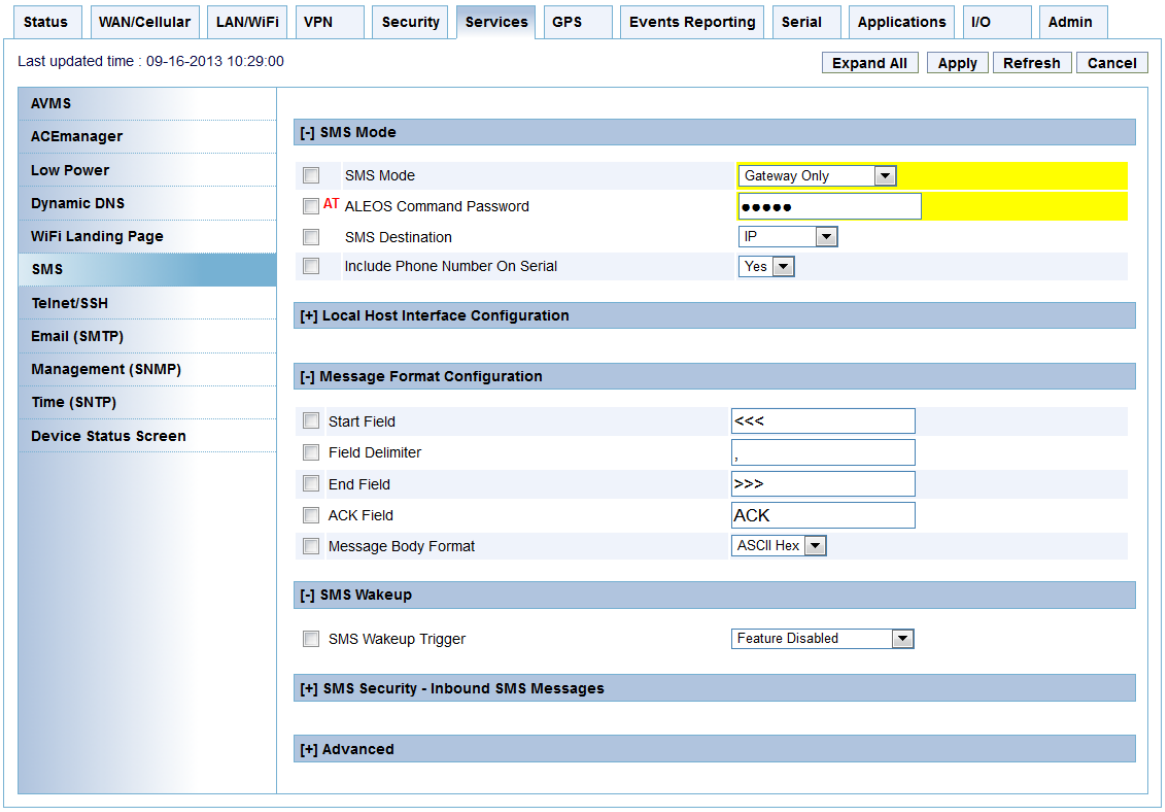


Figure 8-10: ACEmanager: Services > SMS (Gateway Only)

SMS Mode

1. In the SMS Mode field, select Gateway Only.
2. Enter the desired password in the ALEOS Command Password field or leave the field blank to use the default password.

   The password you configure can be any alphanumeric string between 1 and 255 characters long.

   For more information see SMS Password Security on page 171.
3. In the SMS destination field, select from the following options:
   - Serial—Messages are sent to the Serial port on the destination host.

     If you want to include the phone number as part of the information sent to the serial port, select Yes in the Include Phone Number on Serial field.

     Proceed to step 11.
   - IP—Messages are sent using IP. Proceed to step 4.

Local Host Interface Configuration (Only applies if you selected Ethernet in the SMS destination field)

4. Enter the Local Host IP address.

This is the IP address of the attached local host that is used as the destination for all incoming Gateway messages.

5. Enter the Local Host Port.

   This is the UDP port the destination host listens to for incoming messages.

6. Enter the ALEOS port.

   This is the UDP port on which the AirLink device listens for outbound Gateway messages sent from any local host.

Message Format Configuration (Only applies if you selected Ethernet in the SMS destination field)

7. In the Start field, enter the start of message delimiter, or use the default (<<<).
8. In the Field Delimiter field, enter the delimiter to be used between fields in the SMS message, or use the default (,).
9. In the End field, enter the end of message delimiter, or use the default (>>>).
10. In the ACK field, enter the desired acknowledgment message, or use the default (ACK).

    ALEOS provides a message acknowledgment on every SMS message when it is passed to the radio. If ALEOS does not send an ACK, wait for 30 seconds, and then retry.

11. Click Apply.

Sending an SMS Command

The format for sending an SMS command in Gateway Only mode is:
[PW] [Prefix][Command]

Example:

“PW 1234 &&&reset”, where:

- 1234 is the password (required)
  If you did not create a password when you configured SMS, use the default password—the last 4 digits of the SIM number (for SIM-based devices) and the last 4 digits of the ESN (for non-SIM devices). If you do not know the SIM ID or ESN number, you can find it in ACEmanager in Status > WAN/Cellular.
- &&& is the prefix (required)
  Use the default prefix (&&&). The prefix is not configurable in Gateway Only mode.
- reset is the command

For information on sending SMS commands and a list of available commands, see page 377.

Sending a gateway message

The AirLink device acts as an IP gateway to send non-command SMS messages (gateway messages) as UDP packets from a locally-connected host to a configured ALEOS port. The UDP packet must contain the SMS protocol-formatted message.

Note: Do not use the password with gateway messages. The password is only for use with SMS commands.

To create an gateway message:

1. Begin with the start field.
2. Follow with the destination phone number. This number must be in the same format as the phone numbers in the Trusted Phone Number List.
3. Add the field delimiter.
4. Add the data type for the message (ASCII, 8-bit, or Unicode).
5. Add another field delimiter.
6. Add the number of ASCII characters in your message.
7. Add another field delimiter.
8. Add the message to be sent in ASCII hex format. ASCII is case sensitive.
9. Finish with the end field.

   Example: You want to send the following message: “Test message” to phone number (510) 624-4200. To use this feature, convert the message to hex:54657374206d657373616765. Then format the message as follows:

   <<<15106244200,ASCII,12,54657374206d657373616765>>>

   where:
   - “<<<” is the start delimiter
   - “15106244200” is the phone number
   - “,” is the delimiter between fields
   - “ASCII” is the message type
   - “12” is the number of characters in the message
   - “54657374206d657373616765” is the message itself
   - “>>>” is the end delimiter
10. Send the message.

    After your message is sent, you receive an ACK message in the format ACK Field acknowledgment Code ACK Field. For example, if your message was successfully queued to be sent, you receive the message: ACK0ACK.

If you receive an error message, see SMS on page 383 for details.

Control and Gateway

In Control and Gateway mode you can send an SMS non-command (gateway) message to a device, provided you are sending the message from a trusted number. (See Trusted Phone Number on page 171.)

SMS messages received by the device (inbound) are sent on to the configured host. Messages sent by the host to a configured port on the device are sent out as an SMS by the device (outbound). Essentially, the device forwards SMS messages between the cellular radio and the connected host.

You can also send SMS commands in Control and Gateway mode. If you are sending the SMS message from a trusted number, the password is not required. If you are sending it from a non-trusted number, you must use the password.

Configure ALEOS for Control and Gateway mode

1. In ACEmanager, go to Services > SMS.

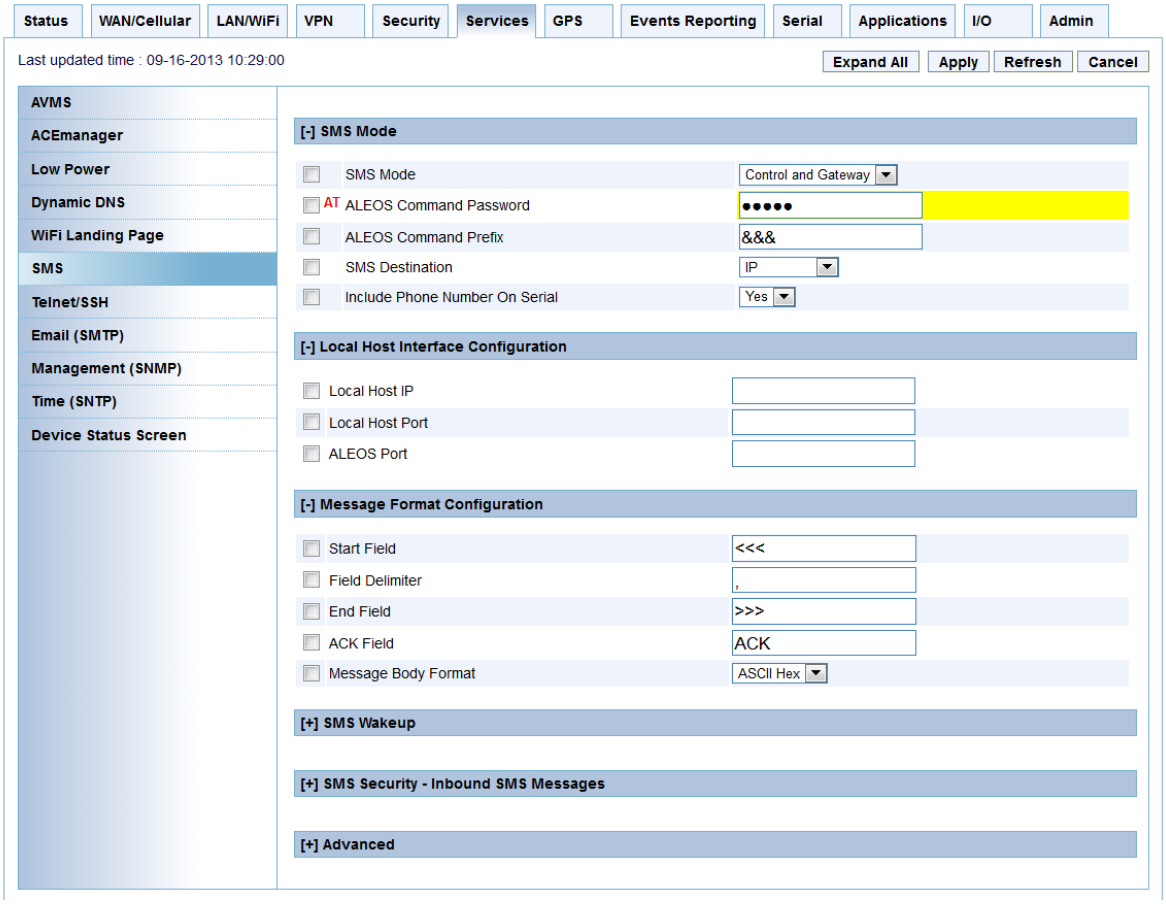


Figure 8-11: ACEmanager: Services > SMS (Control and Gateway)

SMS Mode

2. In the SMS Mode field, select Control and Gateway.
3. Enter the desired password in the ALEOS Command Password field or leave the field blank to use the default password.

   The password you configure can be any alphanumeric string between 1 and 255 characters long.

   For more information see SMS Password Security on page 171.
4. If desired, enter the ALEOS Command Prefix or use the default prefix, &&&.

Note: The ALEOS Command Prefix field in Control and Gateway mode cannot be blank. You must either enter a prefix or use the default. When sending SMS commands in this mode, the prefix must be included.

5. In the SMS destination field, select from the following options:
   - Serial—Messages are sent to the Serial port on the destination host. Proceed to step 14.

- Ethernet—Messages are sent using IP. Proceed to step 5.

Local Host Interface Configuration (Only applies if you selected Ethernet in the SMS destination field)

6. Enter the Local Host IP address.

   This is the IP address of the attached local host that is used as the destination for all incoming Gateway messages.

7. Enter the Local Host Port.

   This is the UDP port the destination host listens to for incoming messages.

8. Enter the ALEOS port.

   This is the UDP port on which the AirLink device listens for outbound Gateway messages sent from any local host.

Message Format Configuration (Only applies if you selected Ethernet in the SMS destination field)

9. In the Start field, enter the start of message delimiter, or use the default (<<<).
10. In the Field Delimiter field, enter the delimiter to be used between fields in the SMS message, or use the default (,).
11. In the End field, enter the end of message delimiter, or use the default (>>>).
12. In the ACK field, enter the desired acknowledgment message, or use the default (ACK).

    ALEOS provides a message acknowledgment on every SMS message when it is passed to the radio. If ALEOS does not send an ACK, wait for 30 seconds, and then retry.

13. Leave the Message Body Format field as ASCII Hex.
14. Click Apply.

Sending an SMS Command

The format for sending an SMS command in Gateway Only mode is:
[PW] [Prefix][Command]

Example:

“PW 1234 &&&reset”, where:

- 1234 is the password
  - If you are sending the SMS command from a trusted number, the password is not required. (See Trusted Phone Number on page 171.)
  - If you are sending the SMS command from a non-trusted number, the password is required.
    If you did not create a password when you configured SMS, use the default password—the last 4 digits of the SIM number (for SIM-based devices) and the last 4 digits of the ESN (for non-SIM devices). If you do not know the SIM ID or ESN number, you can find it in ACEmanager in Status > WAN/ Cellular.
- &&& is the prefix (required)
  This is configurable in Control and Gateway mode.
- reset is the command

For information on sending SMS commands and a list of available commands, see page 377.

Sending a gateway message

The AirLink device acts as an IP gateway to send non-command SMS messages (gateway messages) as UDP packets from a locally-connected host to a configured ALEOS port. The UDP packet must contain the SMS protocol-formatted message.

Note: Do not use the password with gateway messages. The password is only for use with SMS commands.

To create an gateway message:

1. Begin with the start field.
2. Follow with the destination phone number. This number must be in the same format as the phone numbers in the Trusted Phone Number List.
3. Add the field delimiter.
4. Add the message type (ASCII).
5. Add another field delimiter.
6. Add the number of hex characters in your message.
7. Add another field delimiter.
8. Finish with the end field.

   Example: You want to send the following message: “Test message” to phone number (510) 624-4200. To use this feature, convert the message to hex:54657374206d657373616765. Then format the message as follows:

   <<<15106244200,ASCII,12,54657374206d657373616765>>>

   where:

   - “<<<” is the start delimiter
   - “15106244200” is the phone number
   - “,” is the delimiter between fields
   - “ASCII” is the message type
   - “12” is the number of characters in the message
   - “54657374206d657373616765” is the message itself
   - “>>>” is the end delimiter

Note: The gateway message body MUST be in ASCII hex format. ASCII is case-sensitive.

9. Send the message.

   After your message is sent, you receive an ACK message in the format ACK Field acknowledgment Code ACK Field. For example, if your message was successfully queued to be sent, you receive the message: ACK0ACK.

If you receive an error message, see SMS on page 383 for details.

SMS Wakeup

When the AirLink device is in Connect on traffic mode (for details, see Always on connection on page 110), you can configure the AirLink device to also initiate a mobile network data connection on receipt of a specific type of SMS. After the connection is established, it remains active until the configured timeout expires. The a mobile network data connection closes after the specified timeout period. Outgoing traffic sent after the timer is set does not reset the timer.

To configure SMS Wakeup:

1. In ACEmanager go to WAN/Cellular > Advanced and ensure that the Always on connection field is set to Disabled - Connect on traffic.
2. Go to Services > SMS.

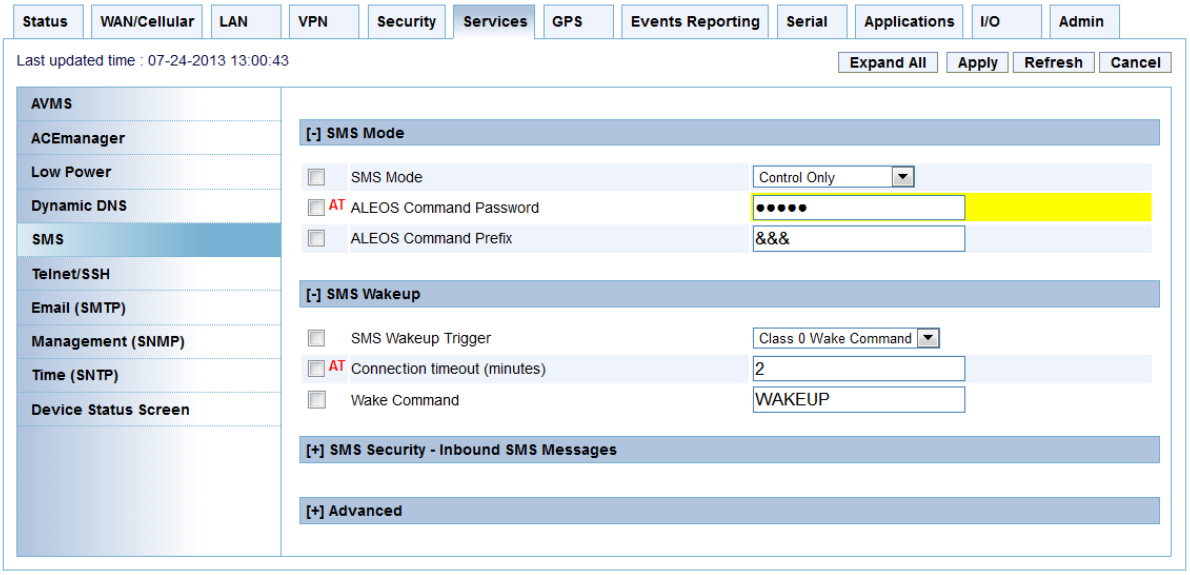


Figure 8-12: ACEmanager: Services > SMS

3. Under SMS Wakeup, select the desired SMS Wakeup Trigger. The options are:
   - Feature Disabled
   - Any Class 0 message
   - Class 0 Wake Command
   - Any SMS message
   - Wake Command

Note: "Class 0 Wake Command" and "Wake Command" are SMS commands. They will not work if SMS mode is "Gateway only" or if the password is missing in "Password only"' mode.

4. Click Apply.
5. In the Connection timeout (minutes) field, enter the number of minutes the mobile network data connection remains active after SMS Wakeup Trigger is received. The default value is 2.

You can also set the Connection timeout using an AT command. For more information, see *SMSWUPTOUT on page 349.

6. If you selected Class 0 Wake Command or Wake Command in step 3, you can specify the SMS command in the Wake Command field or use the default value, WAKEUP. Sending this SMS to the device will wake it up. Example: &&&WAKEUP.
7. Click Apply.

SMS Security

Inbound SMS Messages

Incoming SMS messages are received as UDP packets, and forwarded to the local host IP address and port. The UDP packets are in the same format as sent messages.

When Trusted Phone Number security is enabled, incoming messages coming from the phone numbers in the Trusted Phone Number list are the only ones for which commands will be performed (relay, response etc.) or gateway messages forwarded. Incoming messages from all other phone numbers will be ignored. Commands sent to the device with the correct password are always treated as coming from a trusted number.

All non-alphanumeric characters except a space will be replaced by a dot in ACEmanager.

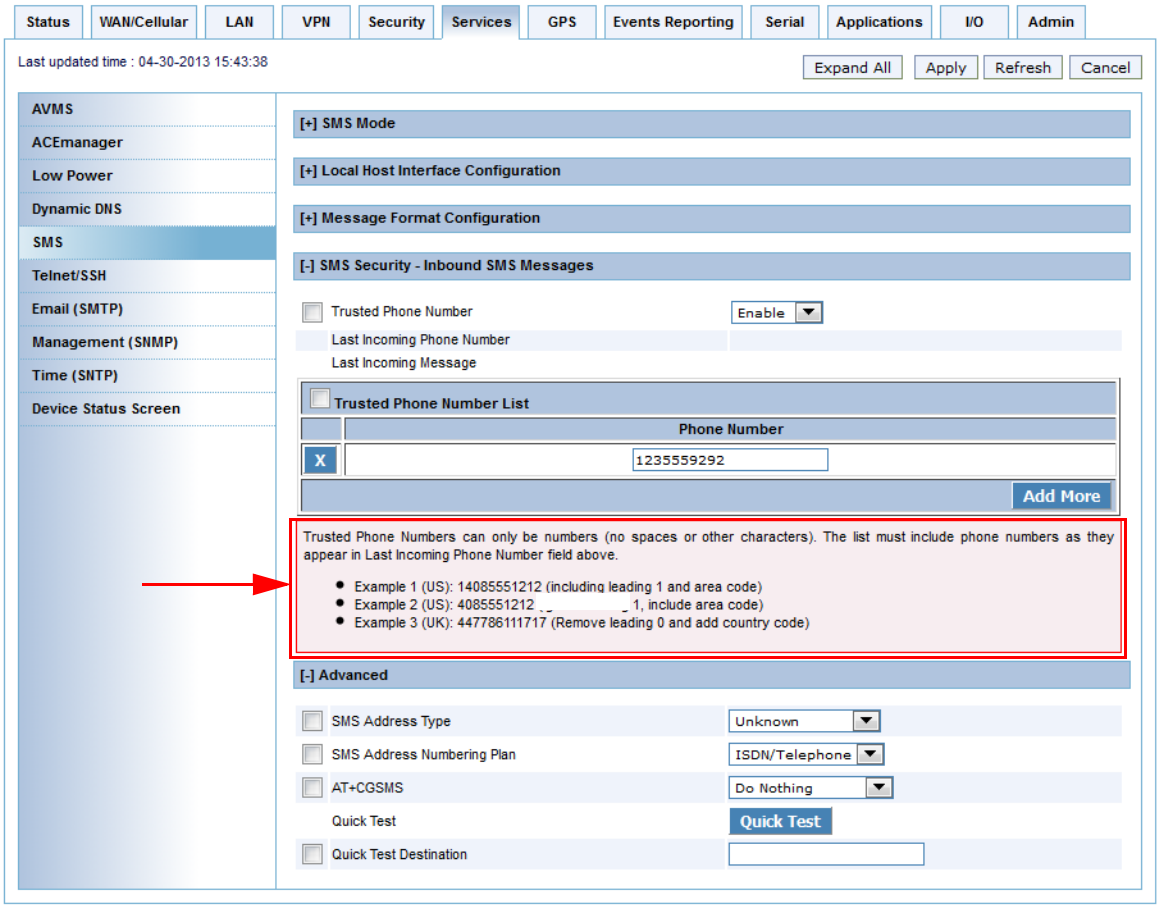


Figure 8-13: ACEmanager: Services > SMS

Field	Description
SMS Security - Inbound SMS Messages	
Trusted Phone Number	Allows you to Enable or Disable a trusted phone number
Last Incoming Phone Number	The last inbound phone number is displayed here. This will only be erased with a reset to defaults.
Last Incoming Message	The last incoming message is the last inbound SMS from the phone number. This will only be erased with a reset to defaults.
Trusted Phone Number List	Trusted phone numbers are listed here

Trusted Phone Number

Follow the instructions below to add a Trusted Phone Number on the SMS page.

1. Send an SMS command to the device, and hit Refresh. If Trusted Phone Number is enabled, and the phone number is not in the trusted list, no action will be performed on the message.
2. Once you have the Last Incoming Phone Number that shows up on the SMS screen in ACEmanager, note the exact phone number displayed.
3. Click Add More to add the Trusted Phone Number. The Last Phone Number will continue to display. Additions to the Trusted Phone Number become effective immediately; no device reboot is needed.

Note: The Trusted Phone number can be up to 15 characters long and must be comprised of numbers only.

Note: Phone Numbers (both trusted and not trusted) will be displayed in the Last Incoming Phone Number field.

4. Enter the Last Incoming Phone Number as the Trusted Phone Number.
5. Click Apply.

Note: Do not enter any extra digits, and use the Last Incoming display as a guide to type the phone number. Use "1" only if it is used in the beginning of the Last Incoming Phone Number.

With Trusted Phone Number enabled, only those SMS messages from Trusted Phone Numbers will receive responses to commands or messages acted on as applicable.

SMS Password Security

The SMS Password feature enables you to use a password to send a command at any time to the device. Even if Trusted Phone Number is enabled, you can send an SMS command from a non-trusted number, provided you include the password.

A default SMS password is generated from the last four characters of the SIM ID (for all SIM-based devices) or the ESN (for devices without a SIM, such those using EV-DO), or you can configure your own SMS password.

Tip: *If you do not know the SIM ID or ESN number you can find it in ACEmanager (*Status > WAN/Cellular).

Note: The SMS password is not the same as the ALEOS password used to access ACEmanager or Telnet/SSH.

To configure the SMS password:

1. Go to Services > SMS > SMS Mode.

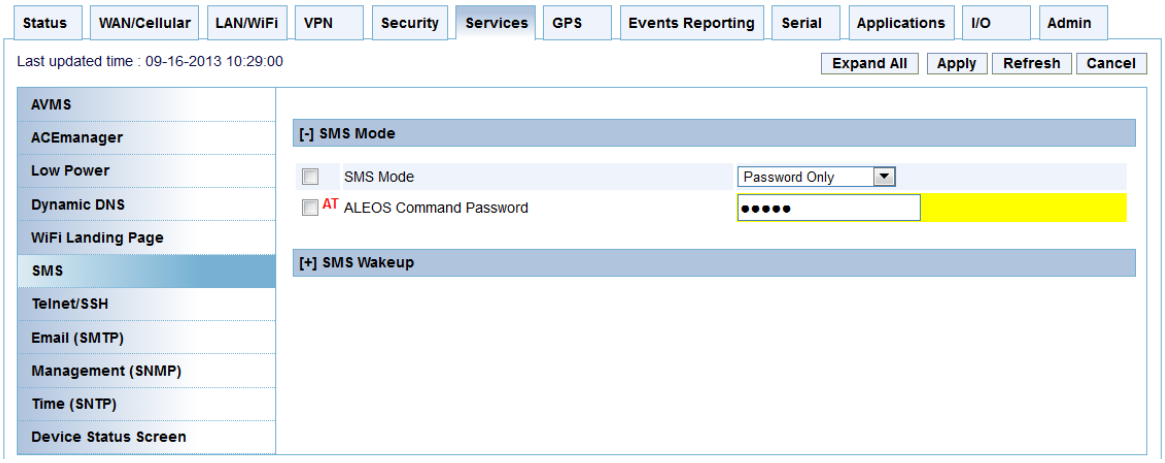


Figure 8-14: ACEmanager: Services > SMS >SMS Mode

2. Enter the desired SMS password in the ALEOS Command Password field.

   The password can be any alphanumeric string with a length between 1 and 255 characters.

3. Click Apply.

Note:

- *The SMS password is not displayed in plain text in ACEmanager. If you want to query it, use the AT command. See *SMS_PASSWORD on page 349.*
- *The SMS password is not cleared by a configuration reset.*
- *If an SMS command is sent with the wrong SMS password, the device replies with a "Wrong Password" message, and the command is dropped.*

Using the Default SMS Password

You can use the default SMS password (last 4 characters of either the SIM ID number for SIM-based devices, or the ESN for devices without a SIM) with no prior configuration.

Note: The default password:

- *Works with all SMS commands*
- *Is not displayed in ACEmanager (If the ALEOS Command Password field is blank, the default password is used.)*
- *Is overridden by a user-defined password*
- *Changes if the SIM is changed, if no user-defined password is configured*

SMS > Advanced

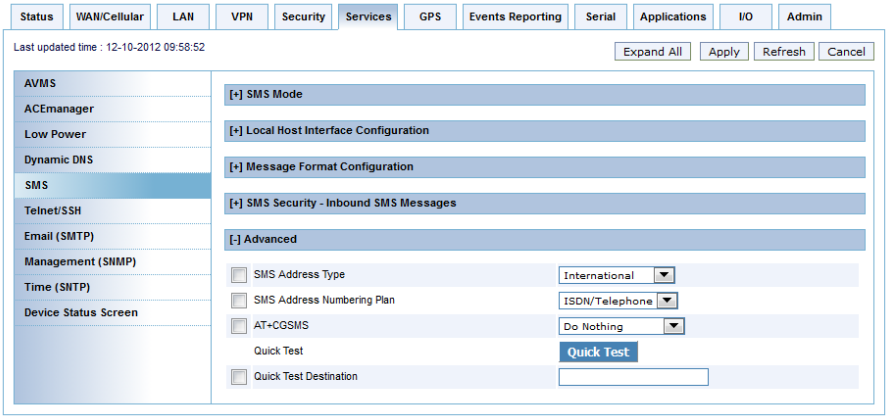


Figure 8-15: ACEmanager: Services > SMS > Advanced

Field	Description
SMS Address Type	For most networks, use the default setting (International). The address type of the phone number used to send outgoing messages and command responses. Options are: • International (default) • National • Network Specific • Subscriber • Abbreviated
SMS Address Numbering Plan	For most networks, use the default setting (ISDN/Telephone). The address numbering plan of the phone number used to send outgoing messages and command responses. Options are: • Unknown • ISDN/Telephone (default) • Date Numbering • Telex • National • Private • ERMES
AT+CGSMS	Allows you to choose the technology used to send SMS messages. For most networks, use the default setting (Do nothing). Options are: • Do nothing (default) • Set AT+CGSMS=0—GPRS • Set AT+CGSMS=1—Circuit switched • Set AT+CGSMS=2—GPRS Preferred (Uses circuit switched if GPRS is not available) • Set AT+CGSMS=3—Circuit Switched Preferred (Uses GPRS if circuit switched is not available) *Note: If your gateway is able to receive SMS messages, but is unable to send them, try changing this field to Set AT+CGSMS=1.*

Field	Description
Quick Test	Allows you to send a test message to the destination entered in the Quick Test Destination field.
Quick Test Destination	Enter the phone number to use for the test message. Click Apply before clicking the Quick Test button. This field is cleared on reboot.

SMSM2M

SMS messages can be sent from the serial command interface. Enter AT*SMSM2M=”[phone] [message]”. The phone number needs to be in the same format as numbers entered in the Trusted Phone Number List.

The message must not exceed 140 characters. To send several messages back to back, you must wait for the OK before sending the next message.

Command	Description
***SMSM2M** ***SMSM2M_8** ***SMSM2M_u**	*SMSM2M is the command for ASCII text. *SMSM2M_8 is the command for 8-bit data. *SMSM2M_u is the command for unicode. Format: *smsm2m=”[phone][ascii message]” *smsm2m_8=”[phone][hex message]” *smsm2m_u=”[phone][hex message]” • The phone number can only consist of numbers (NO spaces or other characters). The phone number should be as it appears in the Last Incoming Phone Number field. Example 1 (US): 14085551212 (including leading 1 and area code) Example 2 (US): 4085551212 (ignore leading 1, include area code) Example 3 (UK): 447786111717 (remove leading 0 and add country code) Command Examples: *smsm2m=”18005551212 THIS IS A TEST” sends in ASCII. *smsm2m_8="17604053757 544849532049532041205445535 4" sends the message “THIS IS A TEST” as 8-bit data. *smsm2m_u="17604053757 000102030405060708090a0b0c0d0e0f808182838485868788898A8b8c8d8e8f" sends the bytes: 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f *Note: Not all cellular carriers support 8-bit or unicode SMS messages.*

Telnet/SSH

Use the Telnet or SSH protocol to connect to any AirLink device and send AT commands.

A secure mechanism to connect remote clients is a requirement for many users. In ACEmanager, Secure Shell (SSH) is supported to ensure confidentiality of the information and make the communication less susceptible to snooping and man-in-the-middle attacks. SSH also provides for mutual authentication of the data connection.

For information on configuring an AirLink device to use SSH PAD mode, see SSH PAD Mode on page 22.

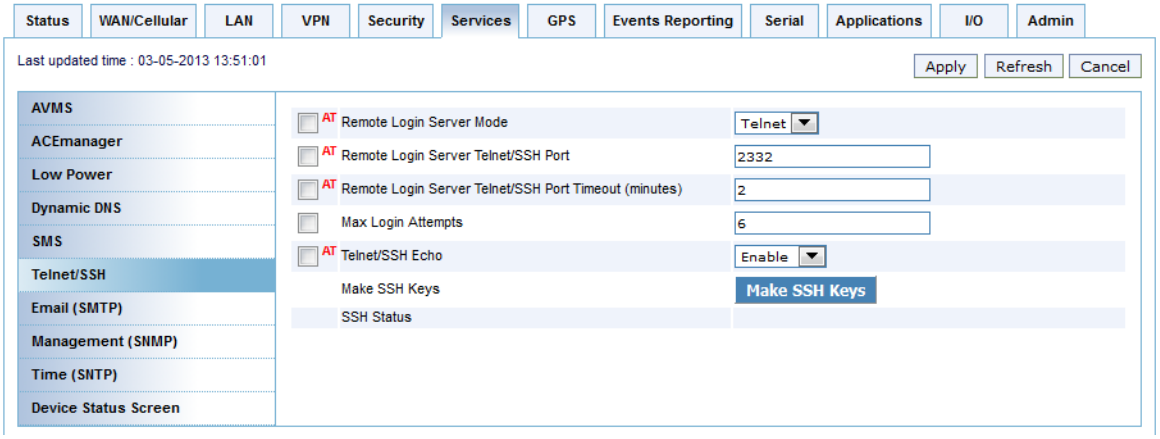


Figure 8-16: ACEmanager: Services > Telnet/SSH

Field	Description
Remote Login Server Mode	Select either Telnet (default) or SSH mode. If you are using this feature to load an application form the ALEOS Application Framework (ALEOS AF), set this option to Telnet.
Remote Login Server Telnet/SSH Port	Sets or queries the port used for the AT Telnet/SSH server. Default: 2332 **Tip:** *Many networks have the ports below 1024 blocked. We recommend that you use a higher numbered port.* After configuring SSH, apply and reset your device.
Remote Login Server Telnet/SSH Port Timeout (mins)	Telnet/SSH port inactivity time out. Default: 2 (minutes)
Max Login Attempts	Sets the maximum number of login attempts. Default: 6
Telnet/SSH Echo	Enable (default) or disable the toggle AT command echo mode.

Field	Description
Make SSH Keys	Creates keys for SSH session applications
SSH Status	Provides the status of the SSH session

Note: When you are connected to SSH locally, you cannot have OTA SSH connected.

Email (SMTP)

For some functions, the device needs to be able to send email. Since it does not have an embedded email server, you need to specify the settings for a relay server for the device to use.

Note: The SMTP function will only work with a mail server that will allow relay email from the ALEOS device's Net IP.

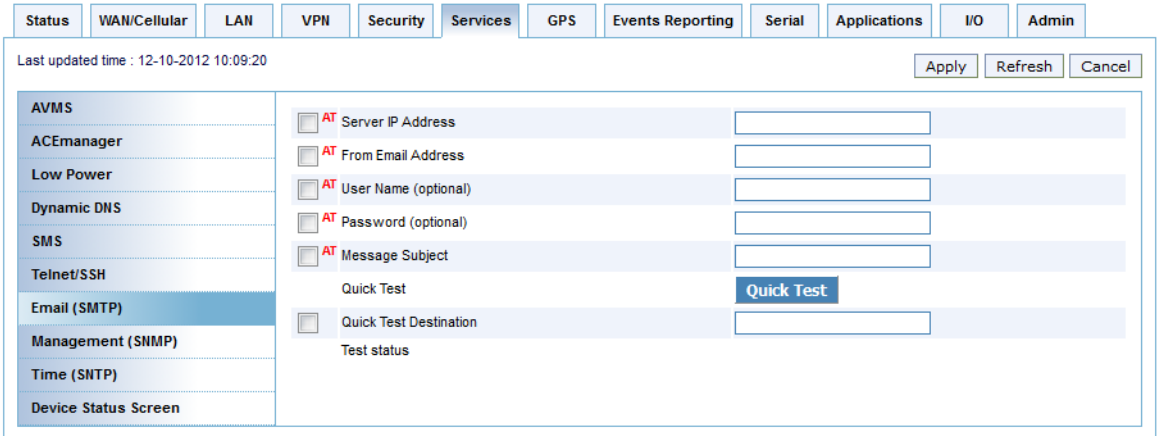


Figure 8-17: ACEmanager: Services > Email (SMTP) — partial screen)

Field	Description
Server IP Address	Specify the IP address or Fully Qualified Domain Name (FQDN) of the SMTP server to use. • d.d.d.d = IP Address • name = domain name (maximum: 40 characters)
From Email Address	Sets the email address from which the SMTP message is being sent. • email = email address (maximum: 30 characters)
User Name (optional)	Specifies the username to use when authenticating with the server

Field	Description
Password (optional)	Sets the password to use when authenticating the email account (*SMTPFROM) with the server (*SMTPADDR). • pw = password *Note: The email server used for the relay may require a user name or password.*
Message Subject	Allows configuration of the default Subject to use if one is not specified in the message by providing a “Subject: xxx” line as the initial message line. • subject = message subject

Management (SNMP)

The Simple Network Management Protocol (SNMP) is designed to allow for remote management and monitoring of a variety of devices from a central location. It is generally used to monitor conditions that may require attention.

The SNMP management system is composed of:

- One or more managers (administrative computers)
- SNMP-compliant devices (such as your AirLink device, a router, a UPS, a web server, a file server, or other computer equipment)
- An agent (data collection software running on the SNMP-compliant devices)
- A Network Management System (NMS) that monitors all the agents on a specific network.

The agent stores information about the device in a Management Information Base (MIB). The manager can send messages to this database to configure and query the status of the device. In addition, the agent running on the device can send traps (unsolicited messages) to the manager on startup, on status change, or when an error condition occurs.

AirLink devices supports SNMPv2c and SNMPv3 and you can configure them as SNMP agents.

Authentication ensures SNMP messages coming from the AirLink device have not been modified and the device cannot be queried by unauthorized users. SNMPv3 uses a User-Based Security Model (USM) to authenticate and, if desired or supported, message encryption. USM uses a user name and password specific to each device.

SNMPv2

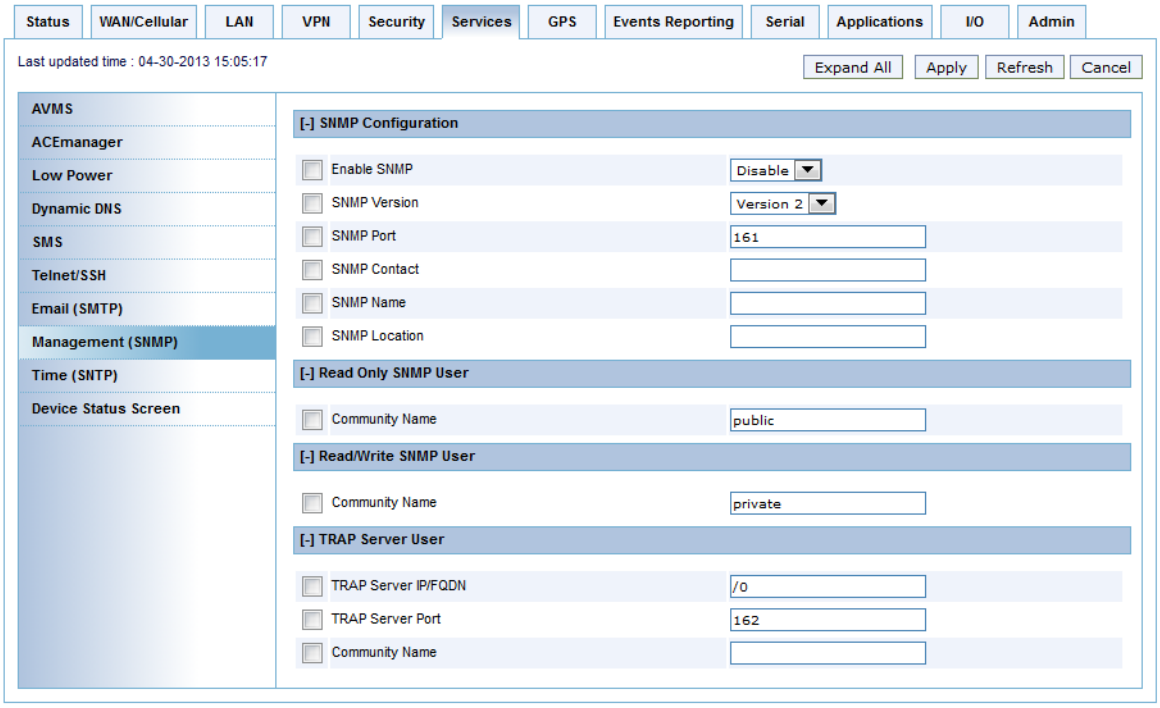


Figure 8-18: ACEmanager: Services> Management (SNMPv2)

Field	Description
SNMP Configuration	
Enable SNMP	Allows you to enable/disable SNMP Default: Disable
SNMP Version	Allows you to select either SNMP protocol Version 2 (default) or Version 3 communications.
SNMP Port	Controls which port the SNMP Agent listens on: • 1–65535 • Default is 161.
SNMP Contact	This is a personal identifier of the contact person you want to address queries to. This is a customer defined field.
SNMP Name	This is the name of the device you want to refer to. This is a customer defined field.
SNMP Location	Location of where your device is stored Enter a meaningful description of where the AirLink device is located.
Read Only SNMP User	

Field	Description
Community Name	The community name is a text string that acts as a password. It is used to authenticate messages that are sent between the management station and the device. Default is public.
Read/Write SNMP User	
Community Name	The community name is a text string that acts as a password. It is used to authenticate messages that are sent between the management station and the device. Default is private.
TRAP Server User	
TRAP Server IP/FQDN	Identifies the IP address or fully qualified domain name (FQDN) of the trap server that the AirLink device sends SNMP traps to
TRAP Server Port	Identifies the specific port the trap server is on • 1–65535 • Default is 162.
Community Name	The community name is a text string that acts as a password. It is used to authenticate messages that are sent between the management station and the device. There is no default value.

SNMPv3

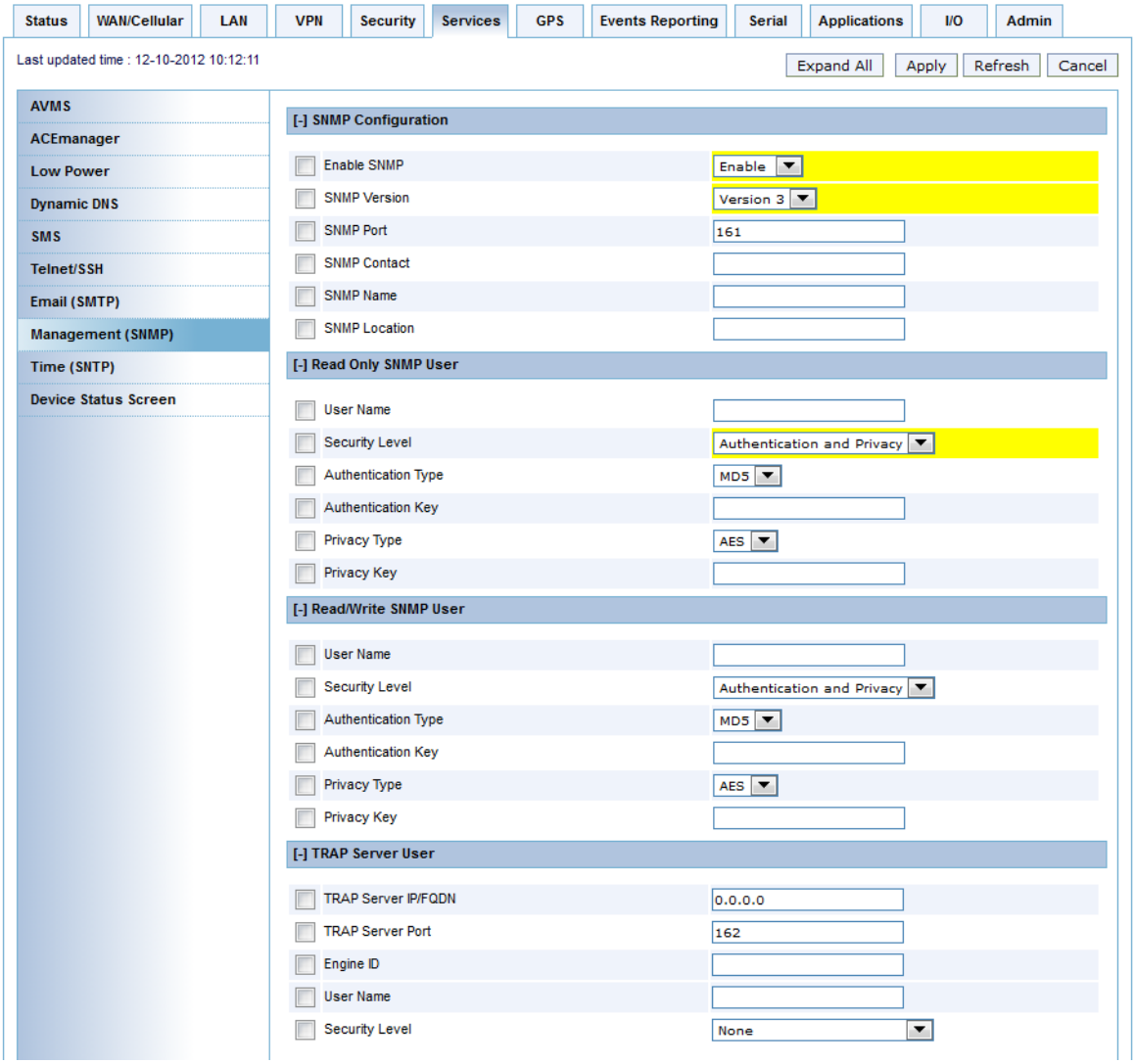


Figure 8-19: ACEmanager: Services> Management (SNMPv3)

Field	Description
SNMP Configuration	
Enable SNMP	Allows you to enable/disable SNMP Default is Disable.
SNMP Version	Allows you to select either SNMP protocol Version 2 (default) or Version 3 communications.
SNMP Port	Controls which port the SNMP Agent listens on: • 1 – 65535 • Default is 161.

Field	Description
SNMP Contact	This is a personal identifier of the contact person you want to address queries to. This is a customer defined field.
SNMP Name	This is the name of the device you want to refer to. This is a customer defined field.
SNMP Location	Location of where your device is stored. This is a customer defined field.
Read Only SNMP	
User Name	Allows these SNMP users to view, but not change the network configuration
Security Level	Security types available: None, Authentication Only, and Authentication and Privacy.
Authentication Type	Authentication types available: MD5 or SHA *Note: This field is only available when you select either Authentication and Privacy, or Authentication Only in the Security Level field.*
Authentication Key	This key authenticates SNMP requests for SNMPv3. • Minimum length: 8 ASCII characters • Maximum length: 255 ASCII characters Example: My Key_1234 *Note: This field is only available when you select either Authentication and Privacy, or Authentication Only in the Security Level field.*
Privacy Type	Privacy types available: AES or DES *Note: This field is only available when you select Authentication and Privacy in the Security Level field.*
Privacy Key	This key ensures the confidentiality of SNMP messages via encryption • Minimum length: 8 ASCII characters • Maximum length: 255 ASCII characters Example: My Key_56789 *Note: This field is only available when you select Authentication and Privacy in the Security Level field.*
Read/Write SNMP For a description of the Read/Write SNMP fields, see Read Only SNMP on page 181.	
TRAP Server User	
TRAP Server IP/FQDN	Identifies the IP address or fully qualified domain name (FQDN) of the trap server that the AirLink device sends SNMP traps to
TRAP Server Port	Identifies the specific port the trap server is on • 1 – 65535 • Default is 162.

Field	Description
Engine ID	The Engine ID is a mandatory field that uniquely identifies the SNMPv3 agent in the device to the server. The Engine ID is 5–32 octets long (1 octet is 2 hex characters). That is: • Minimum length: 10 hex characters • Maximum length: 64 hex characters Create the engine ID by entering hex characters only, with no leading 0x. For example, ABCDEF1020
User Name	See User Name on page 181.
Security Level	See Security Level on page 181.
Authentication Type	See Authentication Type on page 181.
Authentication Key	See Authentication Key on page 181.
Privacy Type	See Privacy Type on page 181.
Privacy Key	See Privacy Key on page 182.

Time (SNTP)

The device can be configured to synchronize its internal clock with a time server on the Internet using the Simple Network Time Protocol. Normally your device will synchronize with the cellular network or GPS.

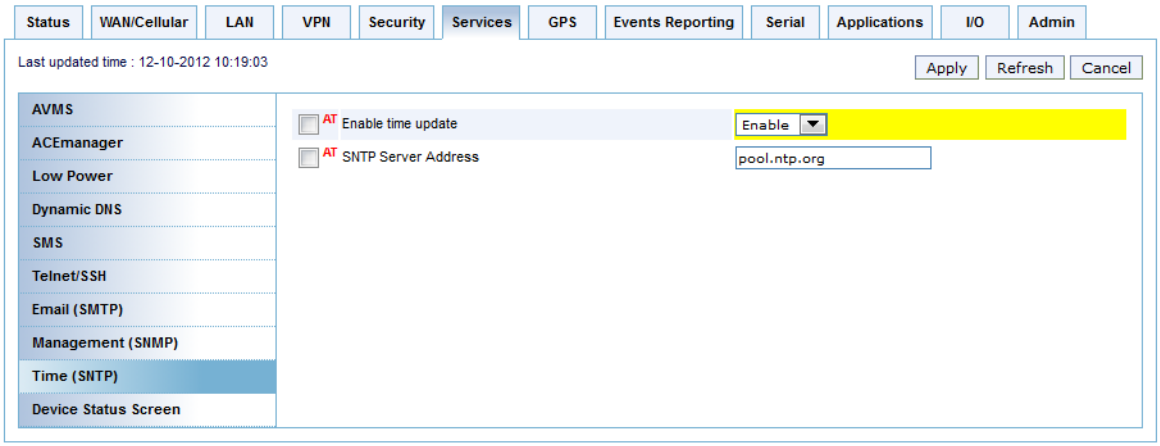


Figure 8-20: ACEmanager: Services > Time (SNTP)

Field	Description
Enable time update	Enables daily SNTP update of the system time. Default: Disable
SNTP Server Address	SNTP Server IP address, or fully qualified domain name, to use if *SNTP=1. If blank, time.nist.gov is used. • d.d.d.d=IP address • name=domain name

Device Status Screen

The Device Status Screen feature, when enabled, allows you to add GPS and network status parameters to the ACEmanager Login screen. Once enabled, subsequent logins to ACEmanager displays whatever status parameters have been previously checked on the Device Status Screen.

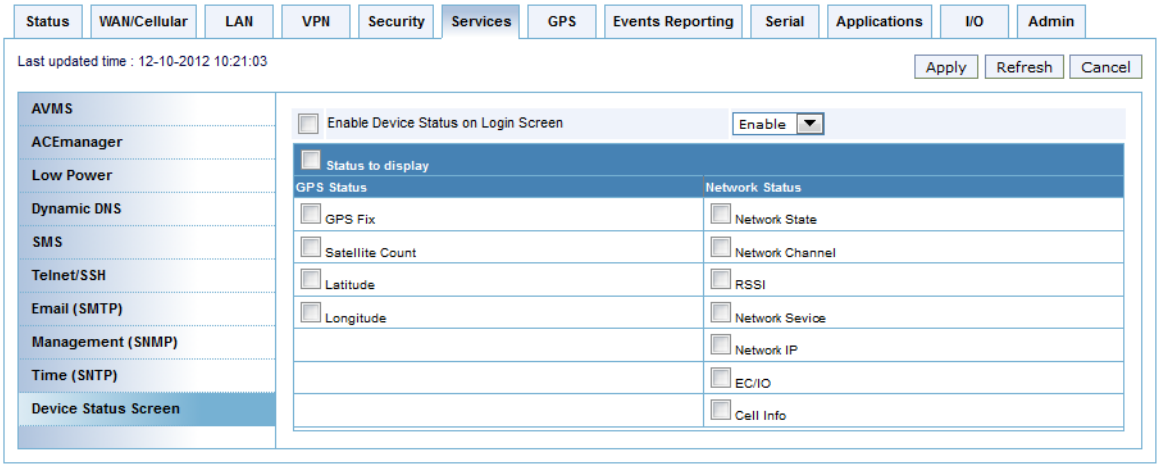


Figure 8-21: ACEmanager: Services > Device Status Screen

Field	Description
Enable Device Status on Login Screen	Enables device status parameters on the login screen Options are: Disable or Enable (default)
Status to display	Allows you to display specific GPS and network status parameters on the login screen

9: GPS Configuration

9

Most AirLink devices are equipped with a Global Positioning System receiver (GPS) to ascertain its position and track the movements of a vehicle or other devices which move. The AirLink device relays the information of its location as well as other data for use with tracking applications.

The AirLink ES440 does not support GPS.

GPS Overview

The Global Positioning System (GPS) is a satellite navigation system used for determining a location and providing a highly accurate time reference.

GPS consists of a “constellation” of 32 satellites in 6 orbital planes. Each satellite circles the Earth twice every day at an altitude of 20,278 kilometers (12,600 miles). Each satellite is equipped with an atomic clock and constantly broadcasts the time, according to its own clock, along with administrative information including the orbital elements of its motion, as determined by ground-based observatories.

A GPS receiver, such as the AirLink device, requires signals from four or more satellites and performs Time Difference of Arrival (TDoA) calculations in order to determine its own latitude, longitude, and elevation.

The GPS data can then be transmitted to a server with a tracking application to compile information about location, movement rates, and other pertinent data.

Note: Depending on the location of the satellites in relation to the device’s location and how many signals are being received, the AirLink device may encounter “GPS drift”, a phenomenon whereby a stationary device is reported as moving by the GPS system. This “drift” is within the location tolerances of the GPS system, but the device may appear to be moving, based on continuous GPS calculations.

Common Uses for GPS

- Driver navigation—The AirLink device provides real time GPS data via the serial or Ethernet port to a local application, including applications that provide mapping and navigation support.
- Automatic Vehicle Location (AVL)—The AirLink device provides real time GPS data to the server that tracks the location and other variables of the vehicle or asset.

ALEOS Supported GPS Report Protocols

- Remote Access Protocol (RAP)

  RAP is a proprietary binary message format developed and maintained by Sierra Wireless and used by many 3rd party applications. Because it is designed and maintained by Sierra Wireless, RAP supports more ALEOS features than other GPS protocols. It is a low-byte-usage protocol that can be used to develop low cost AVL solutions.

  The RAP messages are in hex and are referred to by their message ID. Reports can include GPS data alone, as well as GPS data with the date and time, radio frequency data, radio status information, and I/O state changes, and power state changes. For an example, see GPS RAP Report Sequence Example on page 196. For more information, contact your Sierra Wireless Sales representative for information on how to obtain a copy of the RAP Protocol Guide.
- National Marine Electronics Association (NMEA®)

  NMEA is an ASCII protocol used by many GPS tracking applications.
- Trimble® ASCII Interface Protocol (TAIP)

  TAIP is a digital communication interface based on printable ASCII characters over a serial data link. TAIP was designed specifically for vehicle tracking applications but has become common in a number of other applications, such as data terminals and portable computers, because of its ease of use.
- Xora®

  Protocol specific to Xora asset management and tracking applications

Before Configuring GPS

To decide what configuration you need for your AirLink device, there are some fundamental considerations you should determine:

- **Protocol—**What is the GPS protocol used by your tracking application and what type of reports will you need? (See GPS Report Type on page 191.)
- **Dynamic IP Address—**Does your device have a dynamic IP address and you need to track the specific asset? (See Device ID in Local Reports on page 203.) You can also associate your device with a dynamic DNS configuration. (See Dynamic DNS on page 151.)
- **Server location and type of connection—**Will you be using a local server, a remote server, or both? Will you need a serial or local IP connection? (See Figure 9-1 on page 187 for information.)
- **Multiple GPS servers—**Will you need to have GPS data sent to more than one GPS server?

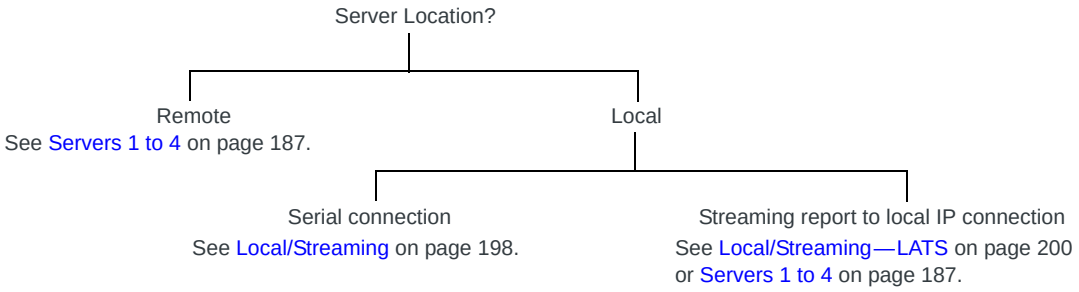

Server Location?
Remote
See Servers 1 to 4 on page 187.
Local
Serial connection
See Local/Streaming on page 198.
Streaming report to local IP connection
See Local/Streaming—LATS on page 200
or Servers 1 to 4 on page 187.

Figure 9-1: Server location and connection type

Note: Most Global settings (described on page 204) apply to remote and local servers. All GPS configuration changes go into effect immediately. No reboot of the AirLink device is necessary. After you configure any settings there is a short pause in receiving GPS reports while the device is re-initialized with the new configuration.

Servers 1 to 4

You can configure up to four servers as report destinations. Each server is configured independently and can be configured to report the same or different information. This enables you to simultaneously receive GPS and other information at more than one location, either local or remote.

The configuration fields are the same for each of the four servers, except that Server 1 has the option to configure one or two redundant servers.

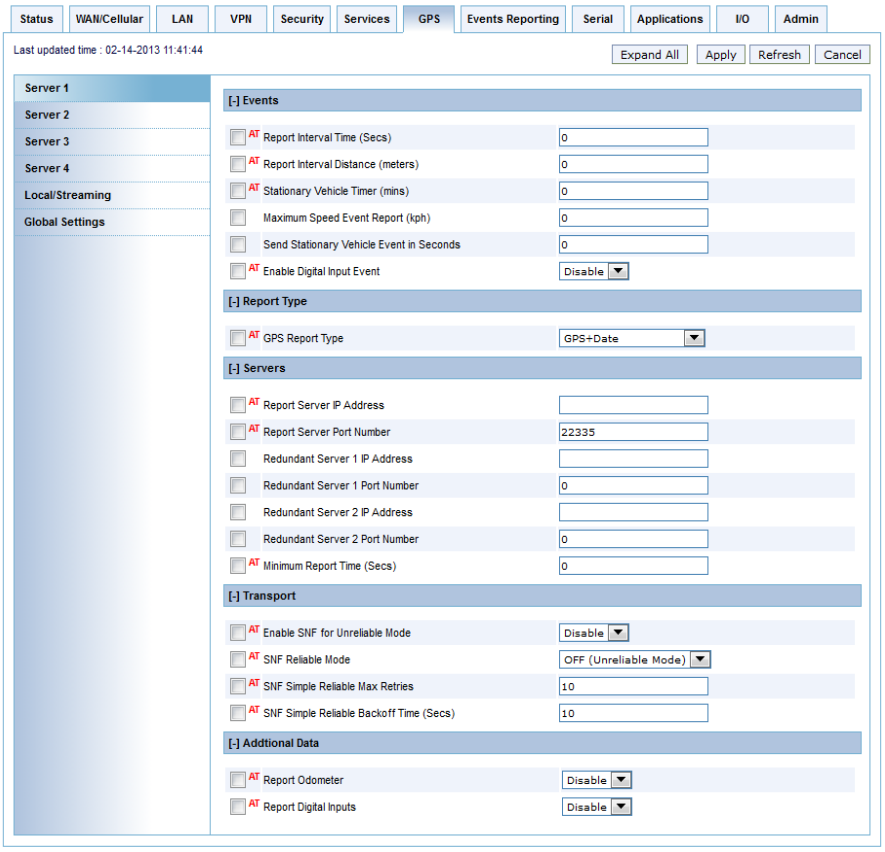


Figure 9-2: ACEmanager: GPS > Server 1

Table 9-1: GPS: Servers 1 – 4

Field	Description
Events — Configure when the GPS reports are sent	
Report Interval Time (secs)	GPS Report Time Interval The amount of time between GPS reports (in seconds) Options are: • 1– 65535 • 0 = Disables GPS reporting based on a time interval (default) With this option disabled, you can still receive reports based on distance traveled or the vehicle being stationary for a configured time. (See Report Interval Distance (meters) on page 189 and Stationary Vehicle Timer (mins) on page 189.) You can also use an AT Command to set this value. For more information, see *PPTIME on page 359. *Note: Your cellular carrier may impose a minimum transmit time.*

Table 9-1: GPS: Servers 1 – 4

Field	Description
Report Interval Distance (meters)	GPS Report Distance Interval in meters The distance (in meters) that the vehicle (or device) travels between sending GPS reports Options are: • 100 – 65535 • 0 = Disables sending GPS reports based on a distance interval (default) With this option disabled, you can still receive reports based on time passed or the vehicle being stationary for a configured time. (See Report Interval Time (secs) on page 188 and Stationary Vehicle Timer (mins) on page 189.) You can also use the AT Command, *PPDISTM, to set this value. For more information, see page 355. *Note: An an additional AT Command, *PPDIST, allows you to configure the GPS report distance interval in 100 meter units. This option is only available through AT Commands. For more information, see page 354.* *Note: If the Report Interval Time and Report Interval Distance fields are both set, a GPS report is sent when the first of the two intervals is reached. For example, if the time interval is reached before the vehicle (or device) has travelled the specified distance, a GPS report is sent based on the time interval. Conversely, if the vehicle (or device) travels the specified distance before the time interval has passed, a GPS report is sent based on the distance interval.*
Stationary Vehicle Timer (mins)	You can use this field if you want to receive less frequent reports when the vehicle is stationary. A GPS report is sent every x minutes the vehicle (or device) is stationary, where x is the value configured in this field. When the vehicle is stationary, this value overrides the value configured in the Report Interval Time field. Options are: • 1–255 • 0 = Disables GPS reporting based on a vehicle being stationary (default) You can also use an AT Command to set this value. For more information, see *PPTSV on page 359.
Maximum Speed Event Report (kph)	A GPS report is sent if the speed (in kilometers per hour) configured in this field is exceeded, and again when the speed goes back down below the configured value. • 0 = Disable (default) • 1 – 255 *Note: If you are using one of the RAP GPS report types (see GPS Report Type on page 191) the GPS report triggered by this feature includes:* • *A marker to indicate that it was triggered by the configured speed being exceeded and when the speed is goes back down below the configured value.* • *The standard GPS information for the configured report type* *For more information, refer to the RAP Protocol Guide.* *If you are not using a RAP GPS report, a standard report is sent.*

Table 9-1: GPS: Servers 1 – 4

Field	Description
Send Stationary Vehicle Event in Seconds	A GPS report is sent if the vehicle (or device) has been in one location for more than the specified time (in seconds) and again when the vehicle (or device) moves from that location. Options are: • 1–255 • 0 = Disables sending GPS reports based on a vehicle being stationary (default) *Note: If you are using one of the RAP GPS report types (see GPS Report Type on page 191) the GPS report triggered by this feature includes:* • *A marker to indicate that it was triggered by the vehicle either being stationary or starting to move again* • *The standard GPS information for the configured report type* *For more information, refer to the RAP Protocol Guide.* *If you are not using a RAP GPS report, a standard report is sent.* You can configure Stationary Vehicle Event in Seconds and Stationary Vehicle Timer together to receive a special report when the device is stationary longer than x seconds, a normal report every x minutes it is stationary (instead of the Report Interval Time) and a special report when the vehicle begins moving again.
Enable Digital Input Event	A GPS report is sent if the configured digital input changes. For example, this could be used to trigger a report being sent when an emergency light or siren is turned on or off, or when a door is opened or closed. The GPS data in the report informs you of where the event took place. Options are: • Disable (default) • Enable *Note: If you are using one of the RAP GPS report types (see GPS Report Type on page 191) the GPS report triggered by this feature includes:* • *A marker to indicate that it was triggered by a change in status of the configured digital input* • *The standard GPS information for the configured report type* *For more information, refer to the RAP Protocol Guide.* *If you are not using a RAP GPS report, a standard report is sent.* You can also use an AT Command to set this value. For more information, see *PPINPUTEVT on page 356.

Table 9-1: GPS: Servers 1 – 4

Field	Description
Report Type	
GPS Report Type	Sets the type of GPS Report Options are: RAP • GPS Data—RAP GPS report that contains only GPS data • GPS+Date—RAP GPS report that contains GPS data with the UTC time and date (default) • GPS+Date+RF—RAP GPS report that contains GPS data, the UTC time and date, and radio frequency information for the cellular connection • GPS+Date+RF+EIO—RAP GPS report that contains GPS data, the UTC time and date, radio frequency information for the cellular connection, and the current I/O state NMEA • NMEA GGA+VTG—NMEA GPS report that contains fix information, vector track, and speed over ground • NMEA GGA+VTG+RMC—NMEA GPS report that contains fix information, vector track, speed over ground, and recommended minimum GPS data • NMEA GGA+VTG+RMC+GSA+GSV—NMEA GPS report that contains fix information, vector track, speed over ground, the recommended minimum GPS data, overall satellite data, and detailed satellite data TAIP • TAIP data—TAIP GPS report that contains position and velocity • Compact TAIP data—TAIP GPS report that contains the compact position • TAIP LN report—TAIP GPS report that contains a long navigation message • TAIP TM report—TAIP GPS report that contains the time and date XORA • XORA data—GPS report used with Xora asset tracking *Note: Only RAP GPS reports can be configured to include odometer and digital I/O information.* *Note: You can also use an AT Command to set this value. For more information, see *PPGPSR on page 356.*

Table 9-1: GPS: Servers 1 – 4

Field	Description
Servers—Configure where the reports are sent	
Report Server IP Address	IP address or FQDN (fully qualified domain name) of the server where GPS reports are sent Example: 192.100.100.100 The IP address can be for a local host or a remote server that is accessed over-the-air or via a VPN tunnel. If an IP with the last octet of 255 is configured (i.e. 192.168.13.255), a report would be broadcast to all IPs on that subnet. When configured to a local host subnet, any connected host would receive the report. *Note: If you want to use it as a LAN host, it must have a private IP address. If you want to use a public IP address, use LATS. (See Local/Streaming—LATS on page 200.)* You can also use an AT Command to set this value. For more information, see *PPIP on page 356.

Table 9-1: GPS: Servers 1 – 4

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Report Server Port Number</td><td>
Destination port on the server where GPS reports are sent
The destination port can be the same for all servers or you can configure a different destination port for each server. Options are: 1–65535
Defaults:

Server 1 destination port: 22335
Server 2 destination port: 22336
Server 3 destination port: 22337
Server 4 destination port: 22338

You can also use an AT Command to set these values. For more information, see *PPPORT on page 358.
Note: If the account is behind a firewall (for example, an account that is not Internet-routable), the report may be redirected to come from a different source port when it arrives at the server.
The source ports on the device are not configurable. The following source ports are used:
<table>
<tr><th>Protocol</th><th>Server</th><th>Port</th></tr>
<tr><td>RAP/NMEA</td><td>1</td><td>17335</td></tr>
<tr><td></td><td>2</td><td>17345</td></tr>
<tr><td></td><td>3</td><td>17346</td></tr>
<tr><td></td><td>4</td><td>17347</td></tr>
<tr><td>TAIP</td><td>1</td><td>21000</td></tr>
<tr><td></td><td>2</td><td>21001</td></tr>
<tr><td></td><td>3</td><td>21002</td></tr>
<tr><td></td><td>4</td><td>21003</td></tr>
<tr><td>XORA</td><td>1</td><td>9494</td></tr>
<tr><td></td><td>2</td><td>9495</td></tr>
<tr><td></td><td>3</td><td>9496</td></tr>
<tr><td></td><td>4</td><td>9497</td></tr>
</table>
</td></tr>
</table>

Table 9-1: GPS: Servers 1 – 4

Field	Description
Redundant Servers — Only available for Server 1 If the redundant server is configured, anytime a report is sent to server 1, an identical report is sent to any configured redundant server(s). Transport/SNF configuration settings do not apply to redundant servers. Commands from redundant servers are ignored. Reports originate from port 17335. The redundant servers can be a local host or a remote server that is accessed over-the-air or via a VPN tunnel.	
Redundant Server 1 IP Address	IP address or FQDN of the first redundant server
Redundant Server 1 Port Number	Port number of the first redundant server The port number can be the same as or different from that of other servers.
Redundant Server 2 IP Address	IP address or FQDN of the second redundant server
Redundant Server 2 Port Number	Port number of the second redundant server The port number can be the same as or different from that of other servers.
Minimum Report Time (secs)	Specifies the minimum time (in seconds) between partial reports or grouped packets being sent You can also use an AT Command to set this value. For more information, see *PPMINTIME on page 357.
Transport / Store and Forward (SNF) — This feature is designed to accommodate periods when the AirLink device is outside the area of cellular network coverage or otherwise unable to reach the report server. Reports are stored and then “forwarded” in a combined packet when the device is again able to contact the server.	
Enable SNF for Unreliable Mode	Store and Forward causes GPS reports to be stored if the AirLink Device goes out of network coverage. Once the device/vehicle is in coverage the stored GPS reports are sent to the server. Options are: • Disable (default)—If there is no cellular network coverage, reports are not stored. • Enable—If there is no cellular network coverage, reports are stored until the AirLink device can access the server. *Note: When you are using GPS and Wi-Fi Client mode: If the Wi-Fi client is connected, reports are sent over the Wi-Fi WAN connection rather than the cellular network. With SNF for Unreliable Mode enabled, if the Wi-Fi WAN connection is active and the cellular connection is not (i.e. out of the cellular coverage area) reports continue to be sent over Wi-Fi. Only if both networks are down are the reports stored and forwarded later when either network is back up.* *Note: You can also use an AT Command to set this value. For more information, see *PPSNF on page 358.*

Table 9-1: GPS: Servers 1–4

Field	Description
SNF Reliable Mode	Store and Forward Reliability: GPS reports are retransmitted if not acknowledged by the server. Options are: • OFF (Unreliable Mode) (default)—If this field is Off, the device does not expect acknowledgment to any GPS report sent to the server. • Reliable Mode—A sequence number (1–127) is added to each packet (window). The server acknowledges every 8th packet. If there is no ACK from the server, ALEOS pings the server and re-sends the packets when the server responds. If the server receives packets out of sequence, the server NAKs the first and last missed packets. ALEOS retransmits the missing packets. • Simple Reliable Mode—ALEOS attempts to contact the server the configured number of times, after which it stops attempting to contact the server and discards messages that cannot be transmitted or received after the configured number of tries. When contacted, the server responds with the ASCII string UDPACK. For information on configuring the maximum number of retries see SNF Simple Reliable Max Retries on page 195. For information on configuring the backoff time, see SNF Simple Reliable Backoff Time (secs) on page 195.) • UDP Sequence Mode—A hex sequence number (30–7f) is prepended to the packet. The server responds with SEQACK and the sequence number. The sequence number is not stored and is re-initialized when the AirLink device is reset or power cycled. Unacknowledged packets are dropped after the configured number of retries. • TCP Listen Mode—This mode is the same as UDP Sequence Mode, except that the server initiates the connection using TCP. Use this mode if your server is behind a firewall. If you are using this mode, the AirLink device must have a mobile terminated/ Internet routable IP address. • TCP—When the AirLink device is out of coverage (no service, the link is down, etc.) reports are stored until the device can access the server. *Note: You can also use an AT Command to set this field. For more information, see *PPSNFR on page 358.*
SNF Simple Reliable Max Retries	When the AirLink device is configured to use Simple Reliable Mode, use this field to set the maximum number of retries when a report is sent and there is no response. Use the SNF Simple Reliable Backoff Time (secs) field to set the interval between retries. Options are: • Disabled • 1–255 retries (Default is 10.) You can also use an AT Command to set this value. For more information, see *PPMAXRETRIES on page 357.
SNF Simple Reliable Backoff Time (secs)	When the AirLink device is configured to use Simple Reliable Mode, use this field to set the interval for the retries. (Use the SNF Simple Reliable Max Retries field to set the maximum number of retries.) • (Default is 10.) You can also use an AT Command to set this value. For more information, see *PPSIMPLETO on page 358.
Additional Data When configured, these options add additional data to RAP reports (see GPS Report Type **on page 191**) sent in response to any trigger.	

Table 9-1: GPS: Servers 1 – 4

Field	Description
Report Odometer	Enables odometer reporting. Options are: • Disable (default) • Enable You can also use an AT Command to set this value. For more information, see *PPODOM on page 357.
Report Digital Inputs	Enables digital input reporting. Options are: • Disable (default) • Enable You can also use an AT Command to set this value. For more information, see *PPREPORTINPUTS on page 358.

Redundant Servers

When one or two redundant servers are enabled, each time a message is sent out to the main server a second identical message is sent to the redundant server(s).

The redundant servers can be running the same or different application than the primary server. The messages to the redundant server are independent of the primary server settings or state.

You can configure one or both redundant servers. The messages are sent independently to either or both.

Note: Messages are sent whether or not the server is available and do not use any reliable mode format. Receipt of a message is not acknowledged nor is any message resent. Messages to redundant servers are in UDP only.

GPS RAP Report Sequence Example

In this example:

The AirLink device is installed in a police car.

- Digital input 2 is connected to the switch that controls the siren.
- Digital input 3 is connected to the laptop docking station.

ACEmanager has the following configuration:

- Report Interval Time: 30 seconds
- Report Interval Distance: 150 meters
- Stationary Vehicle Timer: 5 minutes
- Send Stationary Vehicle Event in Seconds: 6 seconds
- Maximum Speed Event: 100 km/h
- Enable Digital Input Event: Enable
- Report Type: GPS + Date (RAP GPS report type 0x12)
- Low Power Mode: Low Voltage (See Services > Low Power on page Low Power on page 147.)

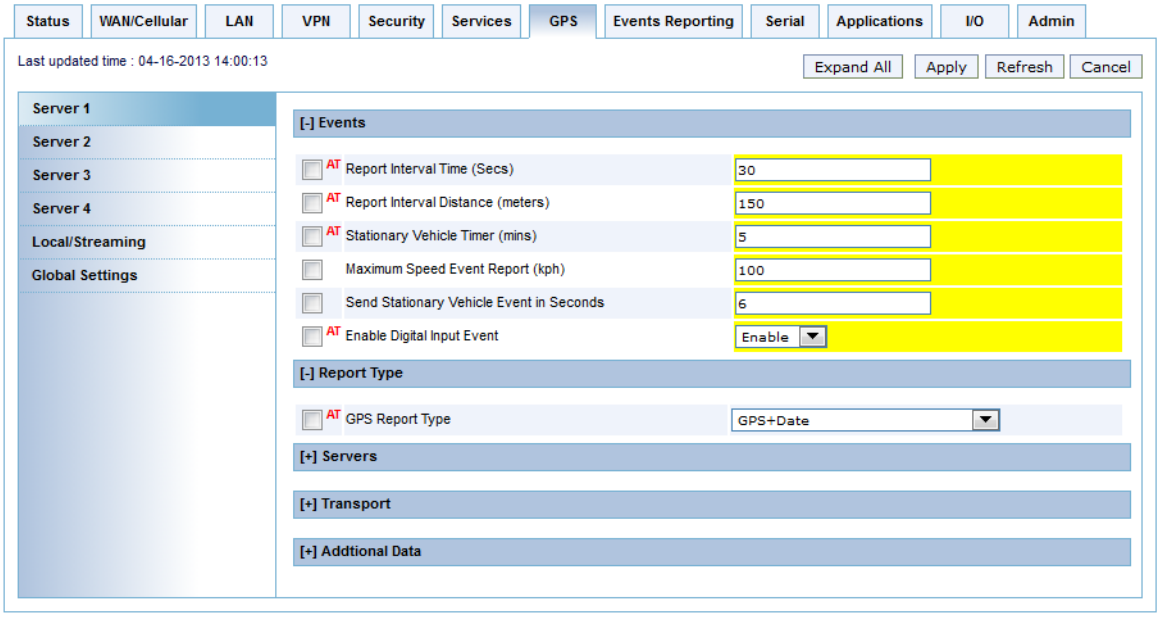


Figure 9-3: GPS > Server 1—Example

The following table provides a sample scenario for this ALEOS configuration.

Event / Action	GPS RAP report sent to the server
The AirLink device in the police car is connected to power for the first time.	A 0x10 (power up) report is sent.
The police car is driving around the patrol area.	A 0x12 (GPS + Date) report is sent every 150 meters or every 30 seconds, whichever is less.
The police officer spots a speeding vehicle, switches on the siren, and pursues the vehicle.	Digital input 2 which is connected to the siren switch is triggered and a 0x27 (DIN 2 changes to 1) report is sent.
The vehicle speeds up, with the police car in pursuit.	When the police car exceeds 100 km/h, a 0x2e (maximum speed exceeded) report is sent. A 0x12 (GPS + Date) report is sent every 150 meters.
The vehicle being pursued and the police car slow down.	When the police car's speed goes below 100 km/h, a 0x2f (return to normal speed) report is sent.
The speeding vehicle pulls over and stops at the side of the road. The police car pulls in behind it. The officer turns off the siren, leaves the engine idling, gets out of the car, and walks over to the other vehicle.	Digital input 2 which is connected to the siren switch is triggered, and a 0x26 (DIN 2 changes to 0) report is sent. Six seconds after the police car comes to a stop, a 0x2c (stationary vehicle event) report is sent. While the car remains stopped with the engine idling, a 0x12 (GPS + Date) report is sent every 5 minutes.
The officer issues a ticket, returns to the police car and drives away.	When the police car is back in motion, a 0x2d (started moving event) report is sent. A 0x12 (GPS + Date) report is sent every 150 meters or 30 seconds, whichever is less.
The police car stops in front of the police station.	Six seconds after the car stops, a 0x2c (stationary vehicle event) report is sent.
The officer disconnects the laptop from the dock.	Digital input 3 connected to the docking station is triggered. A 0x28 (DIN 3 changes to 0) report is sent.

Event / Action	GPS RAP report sent to the server
The officer turns off the ignition.	Before the AirLink device goes into Low Power (sleep) mode, it sends a 0x30 (entering low power mode) report.
The officer on the next shift gets into the car and turns on the ignition.	When the AirLink device wakes up from Low Power mode, it sends a 0x31 (Wake up from Low Power mode event) report.

Local/Streaming

Some in-vehicle/navigation applications accept GPS reports via a serial connection, generally using either NMEA or TAIP. To configure serial streaming for DB-9 (RS-232) ports and/or USB Serial ports, go to GPS > Local Streaming. If you have an AirLink GX Series device with an I/O card installed, you can also use the I/O X-Card serial ports to stream GPS data.

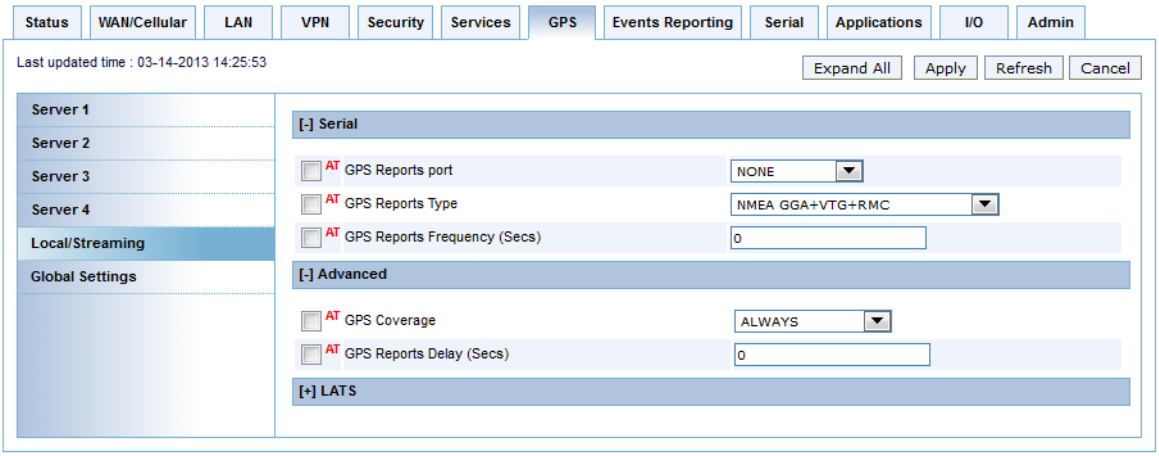


Figure 9-4: ACEmanager: GPS > Local/Streaming

Table 9-2: GPS: Local/Streaming

Field	Description
Serial	
GPS Reports Port	The serial port or USB serial link that reports are sent to Options are: • NONE (default) • DB9 Serial • USB Serial • DB9 and USB • X-Card Serial • X-Card Serial and DB9 • X-Card Serial and USB • X-Card Serial, DB9 and USB You can also use an AT Command to set this value. For more information, see *PGPS on page 353. *Note: If you want to stream GPS data to a USB port, the USB port must be configured on the LAN > USB window to act as a serial port. See USB Device Mode on page 77.* *Note: The X-Card options are only available for a GX Series device with an I/O X-Card installed.*
GPS Reports Type	ASCII text GPS Report type to send via the serial link: • NMEA GGA+VTG+RMC—NMEA GPS report that contains fix information and vector track and speed over ground, and recommended minimum GPS data (default) • NMEA GGA+VTG+RMC+GSA+GSV—NMEA GPS report that contains fix information and vector track and speed over ground, the recommended minimum GPS data, overall satellite data, and detailed satellite data • TAIP data—TAIP GPS report that contains position and velocity • TAIP compact data—TAIP GPS report that contains the compact position • TAIP LN report—TAIP GPS report that contains a long navigation message • TAIP TM report—TAIP GPS report that contains the time and date You can also use an AT Command to set this value. For more information, see *PGPSR on page 354.
GPS Reports Frequency (secs)	How frequently (in seconds) the GPS report is sent to the serial link Options are: • 1–65535—(up to 18.2 hours) You can also use an AT Command to set this value. For more information, see *PGPSF on page 354. *Note: In devices with radio module MC8705, setting this field to 1 sec may result in the device providing GPS locations in intervals ranging from 1 to 3 secs (generally under 2 seconds). To determine which radio module your device has, in ACEmanager go to Status > About and check the Radio Module Type field.*

Table 9-2: GPS: Local/Streaming

Field	Description
Advanced	
GPS Coverage	This field refers to the cellular network coverage. Options are: • ALWAYS (default)—GPS reports are always streamed to the serial link. • Out of Coverage—GPS reports are only streamed to the serial link when the device has no cellular connection. You can also use an AT Command to set this value. For more information, see *PGPSC on page 353. **Tip:** *The Out of Coverage option enables you to use a back-up in-vehicle mapping application that does not rely on cellular network access.*
GPS Reports Delay (secs)	The delay (in seconds) before the out of the coverage stream begins. This field only applies if the GPS coverage field is set to “Out of Coverage”. • 0 (default) • 1–255 You can also use an AT Command to set this value. For more information, see *PGPSD on page 354.

Local/Streaming—LATS

LATS is a local IP report. LATS reports are limited to tethered IP-based LAN hosts (Ethernet, USB/net, DUN, PPPoE). LATS does not have any transport/SNF options. The reports are always sent regardless of cellular coverage.

The destination IP cannot be configured directly. The first connected LAN host is used. If multiple hosts are connected, the priority is the host using the Public IP address, or if all hosts are using Private IP addresses, the priority is:

- Ethernet
- USB
- DUN

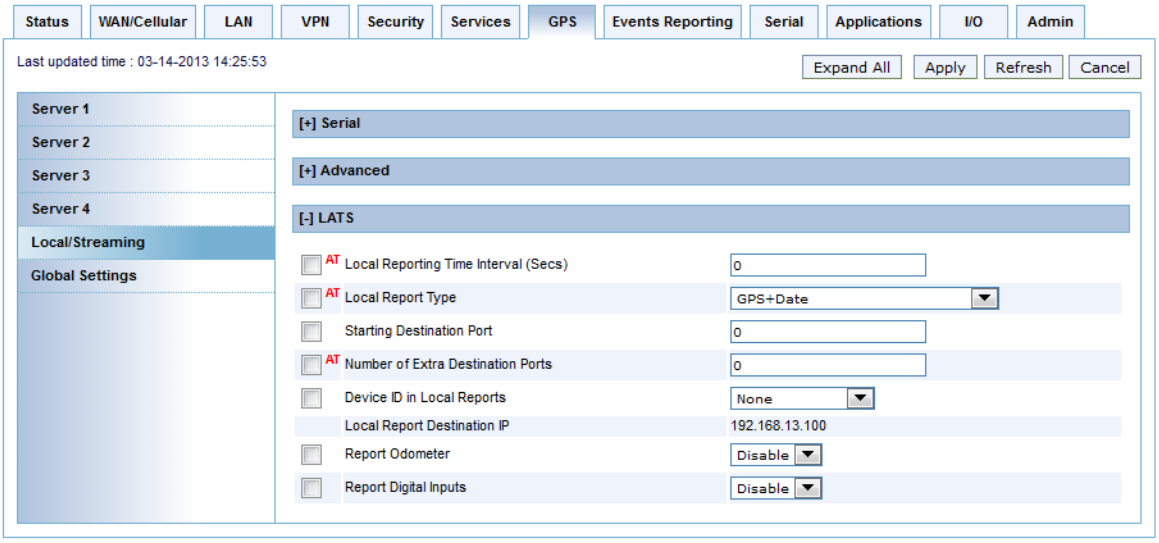


Figure 9-5: ACEmanager: GPS > Local/Streaming: LATS

Table 9-3: GPS: Local/Streaming—LATS

Field	Description
Local Reporting Time Interval (Secs)	The frequency (in seconds) of the reports Options are: • 0 = Disable (default) • 1–255 You can also use an AT Command to set this value. For more information, see *PPLATS on page 356. *Note: If the Local Reporting Time Interval is set to 1 second, there may be some variation in the report interval, with the report interval sometimes being less than 1 second and sometimes more than 1 second. Other settings for this field are accurate.*

Table 9-3: GPS: Local/Streaming—LATS

Field	Description
Local Report Type	Sets one of the following Local Report types: RAP • GPS Data—RAP GPS report that contains only GPS data • GPS+Date—RAP GPS report that contains GPS data with the UTC time and date (default) • GPS+Date+RF—RAP GPS report that contains GPS data, the UTC time and date, and radio frequency information for the cellular connection • GPS+Date+RF+EIO—RAP GPS report that contains GPS data, the UTC time and date, radio frequency information for the cellular connection, and the current I/O state NMEA • NMEA GGA+VTG—NMEA GPS report that contains fix information, vector track, and speed over ground • NMEA GGA+VTG+RMC—NMEA GPS report that contains fix information, vector track, speed over ground, and recommended minimum GPS data • NMEA GGA+VTG+RMC+GSA+GSV—NMEA GPS report that contains fix information, vector track, speed over ground, the recommended minimum GPS data, overall satellite data, and detailed satellite data TAIP • TAIP data—TAIP GPS report that contains position and velocity • Compact TAIP data—TAIP GPS report that contains the compact position • TAIP LN report—TAIP GPS report that contains a long navigation message • TAIP TM report—TAIP GPS report that contains the time and date. *Note: You can also use an AT Command to set this value. For more information, see *PPLATSR on page 357.* *Note: LATS does not have an option for Xora reports.*
Starting Destination Port	The primary port that reports are sent to The LATS source port is 17335. This is not configurable.
Number of Extra Destination Ports	You can send the report to up to 7 additional consecutive ports. For example, if the starting port is 12351 and you set this field to 5, reports are sent to ports 12351, 12352, 12353, 12354, 12355, and 12356. The default is 0 which means only the starting port is used. You can also use an AT Command to set this value. For more information, see *PPLATSEXTRA on page 356.

Table 9-3: GPS: Local/Streaming — LATS

Field	Description
Device ID in Local Reports	Allows use of the IMEI/ESN or phone number in LATS local IP RAP reports to identify a device/vehicle. Options are: • None (default) • Phone Number • ESN/IMEI **Tip:** *Including the device ID is especially useful when your devices have dynamic IP addresses.* *Note: If you want the device ID included in all other RAP GPS reports, see Use Device ID in Location Reports on page 205.*
Local Report Destination IP	This read-only field shows the IP address of the destination that LATS reports are send to. Through its use of DHCP, ALEOS detects if there is a connected host and designates that host's IP as the LATS destination. When no host is connected at startup, ALEOS uses the first IP address in the Ethernet DHCP pool as the destination. When using Public mode for an interface, that interface will be the LATS destination even if it's not the first host connected. *Note: The Local Report Destination IP is not configurable. If you want a GPS report to go to a specific host IP, user Server 1–4 configuration. (See Servers 1 to 4 on page 187.)*
Report Odometer	Enables odometer reporting Options are: • Disable (default) • Enable *Note: Only applies for RAP report types.*
Report Digital Inputs	Enables digital input reporting. Options are: • Disable (default) • Enable *Note: Only applies for RAP report types.*

Global Settings

Most of the Global settings apply to all GPS Server and Local reports.

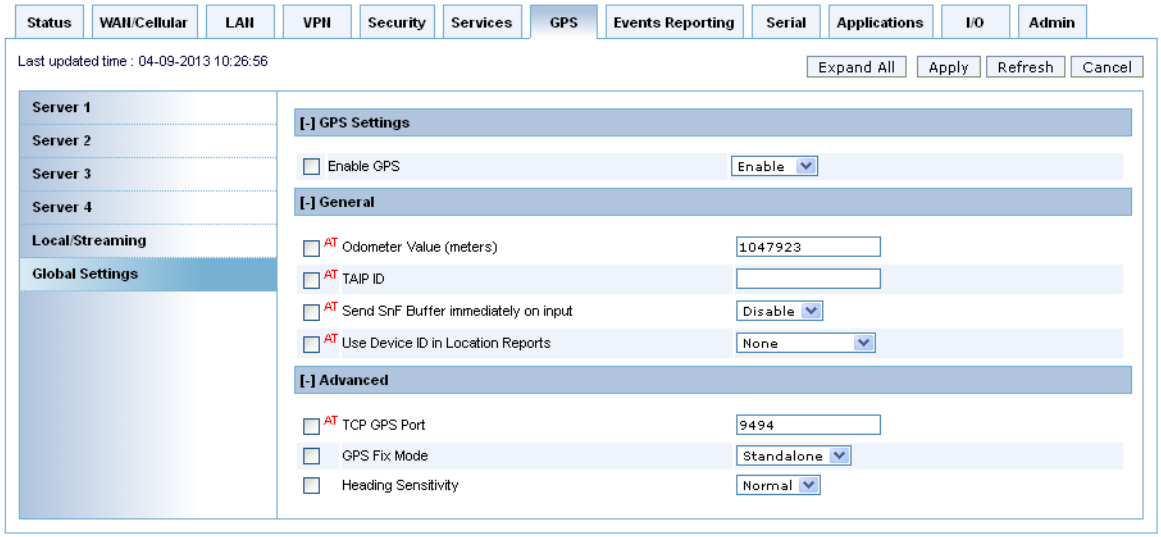


Figure 9-6: ACEmanager: GPS > Global Settings

Table 9-4: GPS: Global Settings

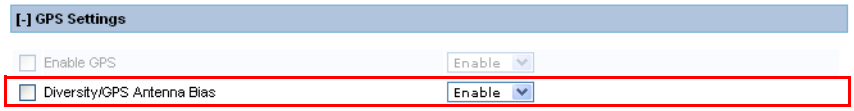
Field	Description
GPS Settings	
Enable GPS	This option only appears on AirLink devices with one of the following radio modules: MC8705, SL8090, and SL8092. (You can view the radio module type on the Status > Home screen.) If your device has one of these radio modules, Sierra Wireless recommends that you disable GPS if you are not using it. Options are: • Enable (default) • Disable
Diversity/GPS Antenna Bias	This field applies only to the LS300.  Configure this field according to the type of GPS antenna you are using. Check the antenna manufacturer's documentation to determine if you have an active or passive GPS antenna. Options are: • Enable (default)—Use the default setting if you are using an amplified (active) GPS antenna. • Disable—Disable this feature if you are using a passive GPS antenna.

Table 9-4: GPS: Global Settings (Continued)

Field	Description
General	
Odometer Value (meters)	The odometer value increments based on the GPS distance traveled. You can include this value in RAP GPS reports. (See GPS Report Type on page 191). You can set the odometer value to an initial value. Maximum value is 4 294 967 295 meters (4,294,967 kilometers or 2,668,769 miles). Default: 0 *Note: The RAP report displays the odometer value in 100s of meters.* You can also use an AT Command to set this value. For more information, see *PPODOMVAL on page 357.
TAIP ID	The four character alphanumeric ID used in all TAIP reports You can also use an AT Command to set this value. For more information, see *PPTAIPID on page 358.
Send SnF Buffer immediately on input	If this feature is enabled, any pending stored reports are sent if the I/O input changes, a stationary vehicle is moved, or a maximum speed is exceeded, provided those events are enabled on the GPS > Server > Events screen. Options are: • Disable (default) • Enable You can also use an AT Command to set this value. For more information, see *PPFLUSHONEVT on page 355.
Use Device ID in Location Reports	Allows use of the IMEI/ESN or phone number in RAP reports configured for Servers 1–4 to identify a device/vehicle. Options are: • None (default) • Phone Number • ESN/IMEI You can also use an AT Command to set this value. For more information, see *PPDEVID on page 355. **Tip:** *Including the device ID is especially useful when your devices have dynamic IP addresses.* *Note: The device ID in RAP reports is in hex, not plain text.* *Note: This option does not apply to LATS reports. If you want the device ID included in LATS GPS reports, see Device ID in Local Reports on page 203.* *Note: If you want this Device ID included in the TCP PAD connections, enable the Include Device ID on TCP Connect field on the Serial screen (Serial > Port Configuration > TCP). See Port Configuration on page 221.*

Table 9-4: GPS: Global Settings (Continued)

Field	Description
Advanced	
TCP GPS Port	You can obtain a single location snapshot from the device via a TCP session using the AirLink device's IP address and the device port configured in this field. • 1–65535 (default 9494) • 0 = Disable You can also use an AT Command to set this value. For more information, see *PPTCPPOLL on page 359. *Note: Access is restricted to the IP address defined for server 1. (See Report Server IP Address on page 192.)*
GPS Fix Mode	Specifies the GPS fix mode. Options are: • Standalone (default) • MS Based—(Mobile Station Based fix) Uses assistance GPS data from a remote server over the WAN interface
Heading Sensitivity	Sets the sensitivity of the GPS heading reading • Normal (default) • High It is recommended that you leave the field set to Normal to avoid showing misleading heading values from poor GPS signal (poor sky view, reflections in urban canyon, etc.), but if your GPS application has its own GPS heading sensitivity algorithms, try changing this setting to High.

10: Events Reporting Configuration

10

Introduction

Events Reporting allows you to generate reports or perform actions in response to the events that are configured in the ALEOS software.

An Event is a measurement of a physical property AND a state change or a threshold crossing. For example, radio module signal strength (RSSI) is a physical property. A threshold crossing could be set to -105 dBm. You can configure an Event which consists of the RSSI with the -105 dBm threshold. There are many Events that can be configured; these are described in detail below.

An Action is an activity which can be performed, such as sending a report to a remote server, sending an SNMP trap, changing the value on a digital signal line, or turning off cellular communication with any devices connected to a host port. If a report is to be sent, you can select the data to include in the report.

Events and Actions work together. When an Event is triggered, this means that, for the physical property being measured, the state change or the threshold crossing has occurred. The Event will then effect the Action to occur. For example, if you have configured an RSSI Event, then you can have a report sent (example: SMS Message) once the threshold is crossed. This relationship is shown conceptually in Figure 10-1.

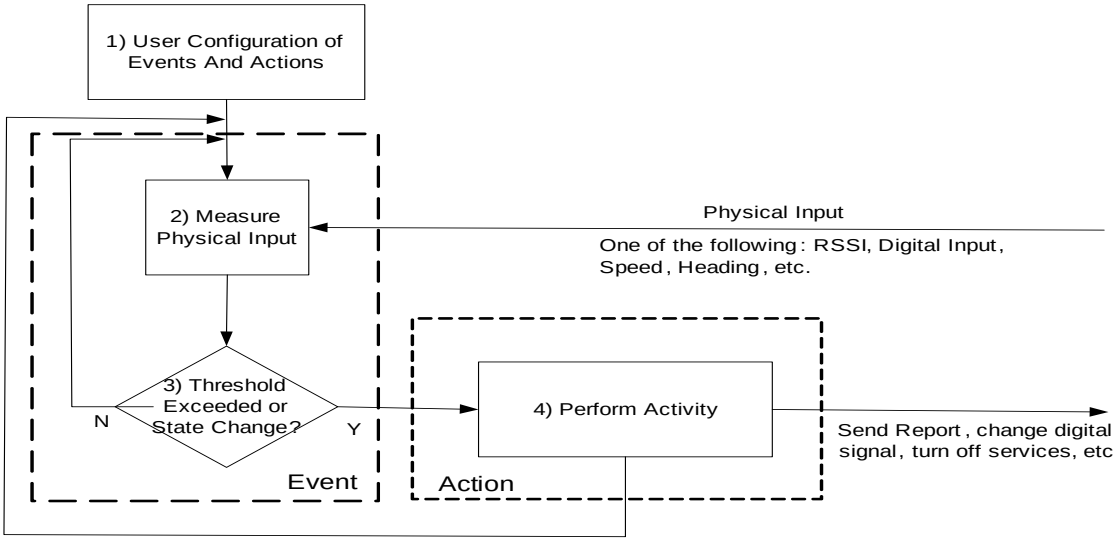

1) User Configuration of Events And Actions
2) Measure Physical Input
Physical Input
One of the following: RSSI, Digital Input, Speed, Heading, etc.
3) Threshold Exceeded or State Change?
N
Y
4) Perform Activity
Send Report, change digital signal, turn off services, etc
Event
Action

Figure 10-1: Events Reporting Concept

The procedure of how Events Reporting works is described below:

1. Configure the events and actions.

2. After deployment, the device begins measuring a physical input.
3. The measurement is compared to the user-configured threshold or state change. If there is no change, then another measurement is performed. If a state change (or threshold crossing) occurs, then the flow moves to step 4.
4. The Action associated with the Event. In this step, a report may be generated, or some other activity is performed. Afterwards, the flow returns to step 1.

Additional Behavior and Features

Events/Actions are not one shot activities. After an Action is performed, the Event is still active and will trigger the next time the state change or threshold crossing occurs.

A single Event may activate one or more Actions. For example, if RSSI is below threshold, you can turn off data services (Action 1) and send an SMS message (Action 2).

A single Action may be activated by one or more Events. For example, if the vehicle speed is above a threshold or if the vehicle heading changes, either Event can perform the same action.

After defining an Event, always select the Apply button to save these definitions and apply them to an Action.

Selecting the Delete button on the Events Reporting tab will delete all current Event and Action data.

Configuration Overview

To configure Events and Actions, complete the following steps:

Note: All Events Reporting configuration changes take effect after a short delay (about one minute). No reboot of the AirLink device is necessary.

1. Define an Event – Events can be configured using the ACEmanager user interface. Select the Events Reporting Tab, and then select the *Add New* subtab to add an event (e.g., RSSI).

Note in the Action Description frame that there are no actions listed.

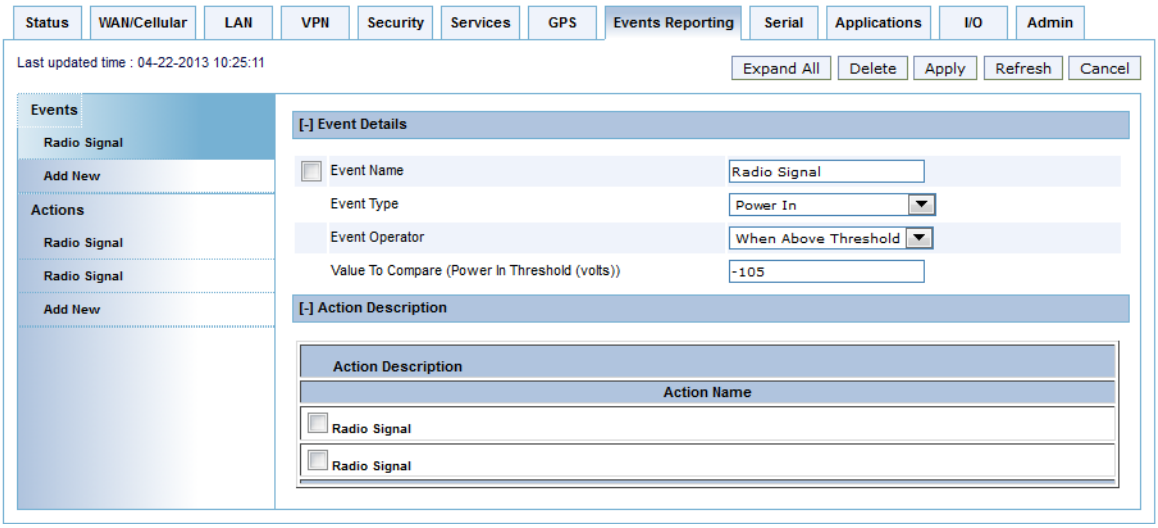


Figure 10-2: ACEmanager: Events Reporting > Events > Add New

2. Define an Action – This is done on the Actions group.

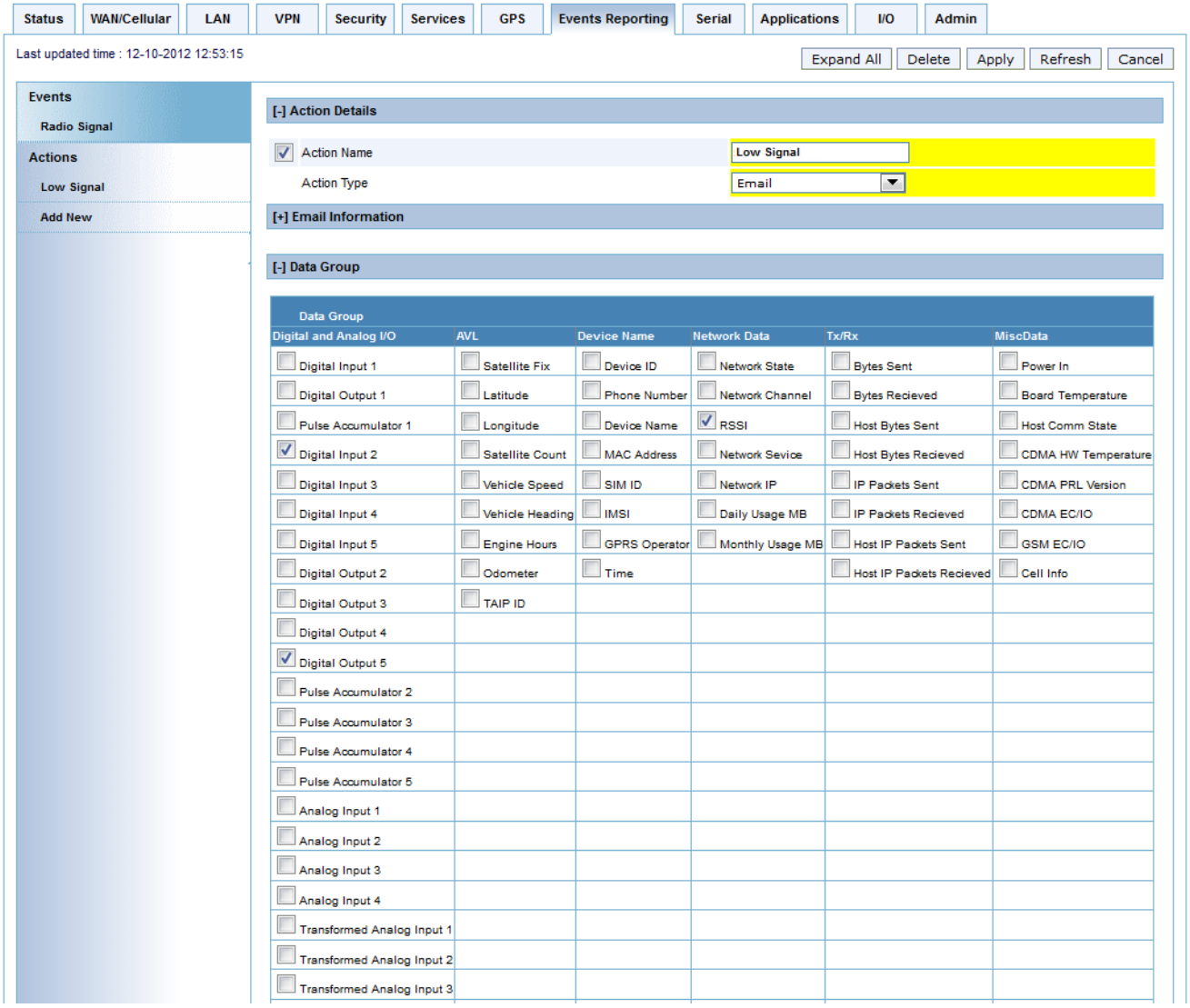


Figure 10-3: ACEmanager: Events Reporting > Actions > Add New

3. Associate the Action with the Event – This is done by clicking on the Events group. On the Events page, note that the new Action (Low Signal) is displayed in the Action Description frame. You can select the check box to associate this action with the Radio Signal Event.

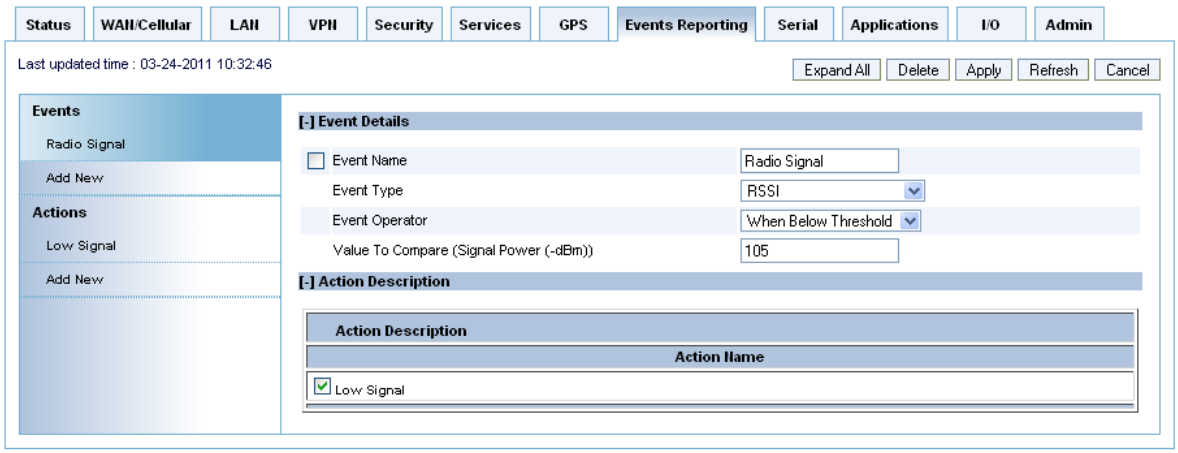


Figure 10-4: ACEmanager: Events Reporting > Events > Cell Radio Sign

4. Click Apply.
5. Click Actions.
6. To send a test report, wait about 1 minute after you click Apply, and then click the Test report button.

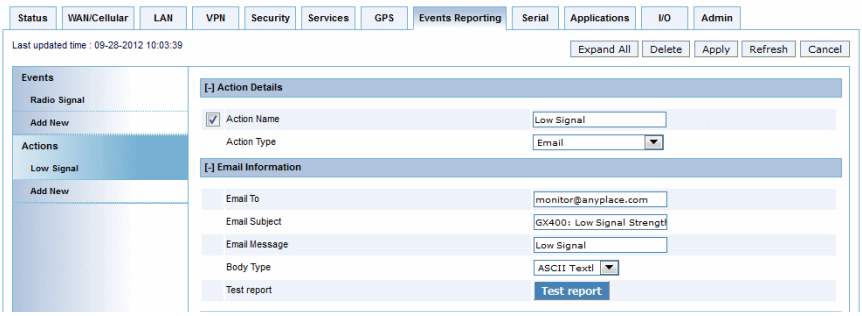


Table 10-1: Event Types

Event Name	Event Type	Threshold or State Change Options
Digital Inputs		
Digital Input # The number of digital inputs depends on the device and in the case of the GX Series device, whether or not you have an I/O X-Card installed.	State Change	Switch Closed Switch Opened On any change
Pulse Accumulator # The number of pulse accumulators depends on the device and in the case of the GX Series device, whether or not you have an I/O X-Card installed.	Threshold Crossing	When Changed By

Table 10-1: Event Types (Continued)

Analog Input # *Note: The number of analog inputs depends on the device and in the case of the GX Series device, whether or not you have an I/O X-Card installed.*	Threshold Crossing	When value crossed above a threshold, below a threshold, or either (volts)
Transformed Analog # *Note: The number of transformed analogs depends on the device and in the case of the GX Series device, whether or not you have an I/O X-Card installed.*	Threshold Crossing	When value crossed above a threshold, below a threshold, or either (units configured on the I/O screen) See Transformed Analog on page 258.
AVL		
GPS Fix	State Change	Fix Lost Fix Obtained Any Fix Change
Vehicle Speed	Threshold Crossing	Vehicle Speed (KM/h)
Heading Change	Threshold Crossing	Heading Change (degrees)
Engine Hours	Threshold Crossing	Engine Hours
Network		
RSSI	Threshold Crossing	Signal Power (-dBm)
Network State	State Change	When Device is Ready
Network Service	State Change	• Roaming • 2G Service • Rev A or HSUPA • Any Data Service
Other Report Types		
Periodic Reports	Threshold Crossing (Time)	Period to compare (seconds)
Power In	Threshold Crossing	Power threshold (volts)
Board Temperature	Threshold Crossing	Degrees Celsius
CDMA HW Temperature	Threshold Crossing	Degrees Celsius
Data Usage		
Daily Data Usage	Threshold Crossing	Percentage of daily threshold
Monthly Data Usage	Threshold Crossing	Percentage of monthly threshold

Note: ALEOS Data Usage is approximate and should not be compared with data usage recorded by the Mobile Network Operator.

SIERRA WIRELESS IS NOT RESPONSIBLE FOR DATA OVERAGES.

Action Description

Select a name for the action of your choice.

Action Type

Under the Events Reporting Action tab, there is an Action Type field which has different parameters listed in the scroll-down menu.

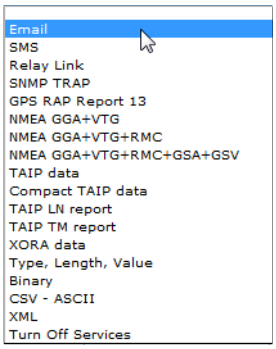


Figure 10-5: ACEmanager: Events Reporting > Action > Action Type scroll down

There are several ways to send a report. The configuration will vary.

- Email
  - Destination email address
  - Subject, Message
  - Data groups
- SMS text message
  - Destination Phone number
  - Message
  - Data Groups

You can configure a maximum of 5 actions per event. If the action requires an IP connection, the following source ports are used. These are not configurable.

Actions (in the order configured)	Source port
Action 1	17348
Action 2	17349
Action 3	17351

Actions (in the order configured)	Source port
Action 4	17352
Action 5	17353

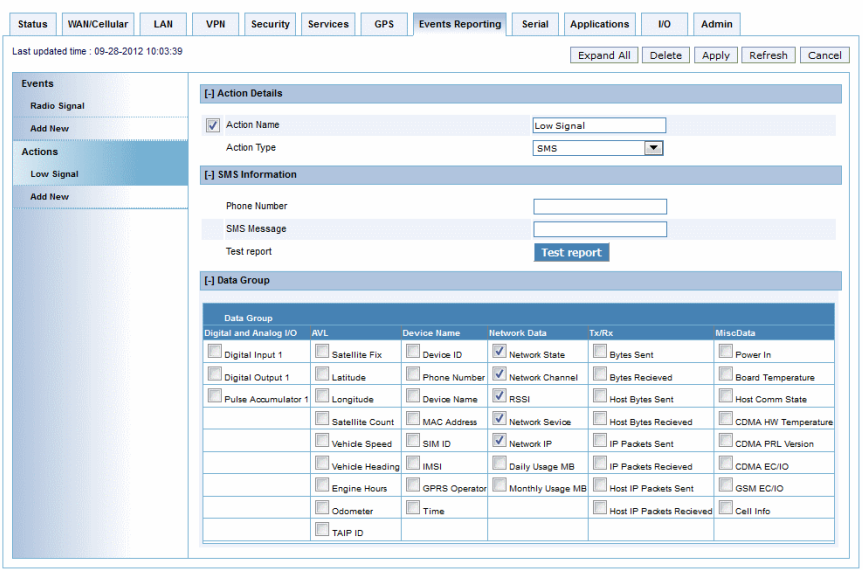


Figure 10-6: ACEmanager: Events Reporting > Action Type > Email (similar fields for SMS)

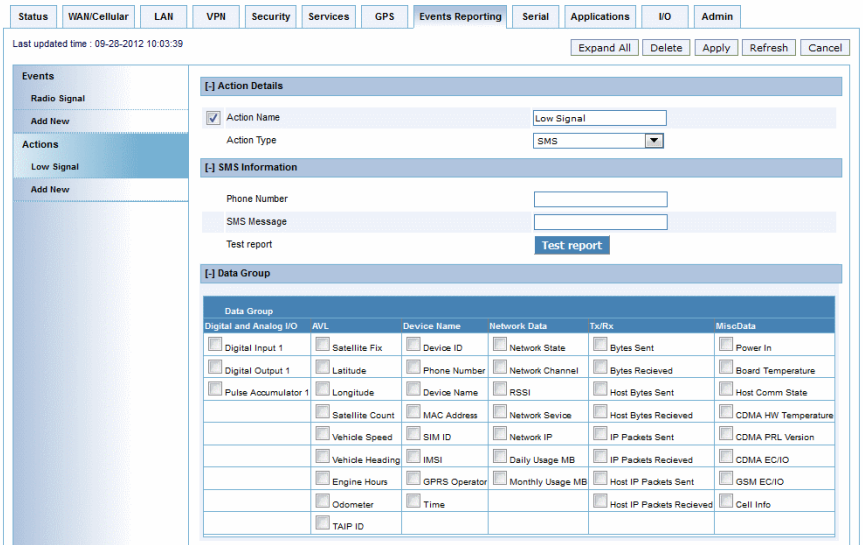


Figure 10-7: ACEmanager: Events Reporting > Action Type > SMS

- SNMP Trap notification
  - Destination IP is configured in the SNMP menu.

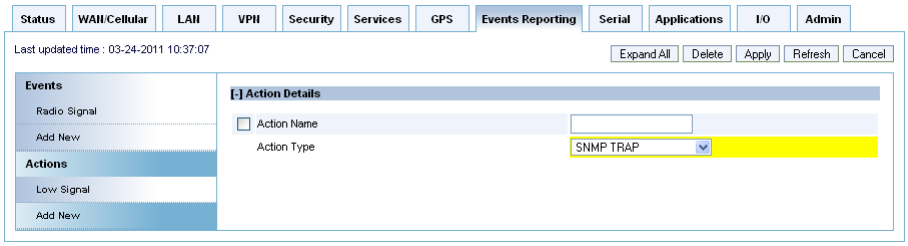


Figure 10-8: ACEmanager: Events Reporting > Action Type > SNMP TRAP

- Relay Link
  - Select the relay to link to, and invert if necessary.

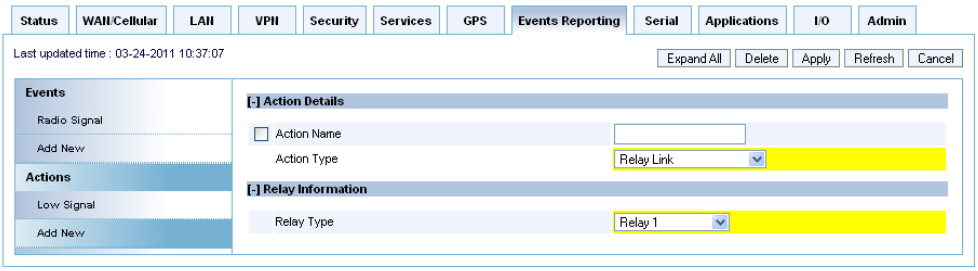


Figure 10-9: ACEmanager: Events Reporting > Action Type > Relay Link

- GPS RAP/Report 13 message
  - Configure the report server store and forward properties and report options.

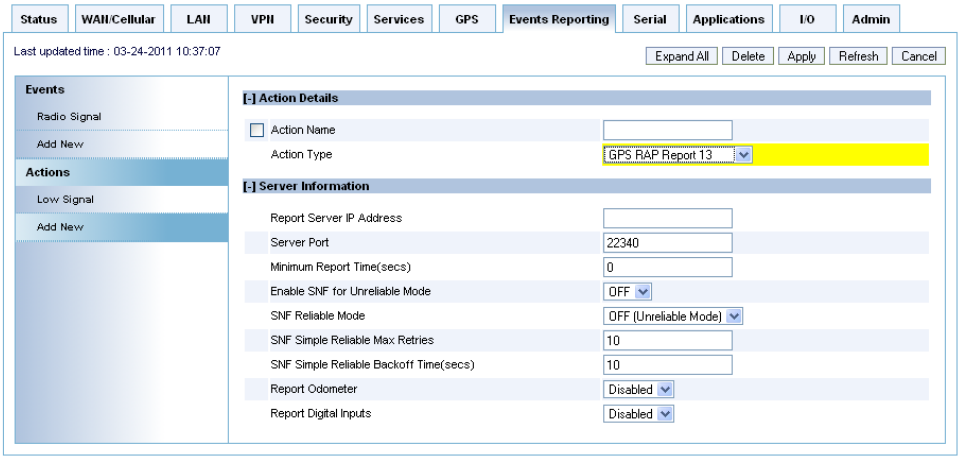


Figure 10-10: ACEmanager: Events Reporting > Action Type > GPS RAP Report 13

- Events Protocol message to a server
  - Destination report server is configured
  - Report format – TLV (Type, Length and Value), Binary, ASCII, or XML.

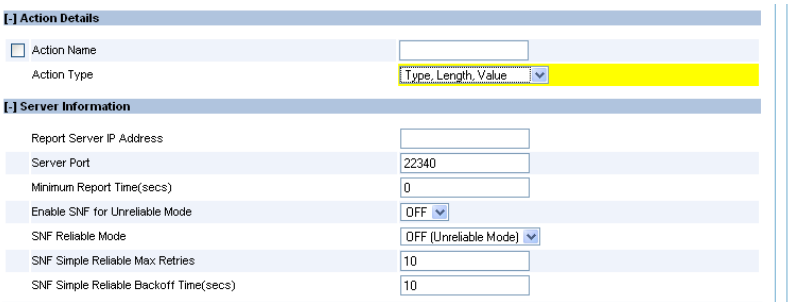


Figure 10-11: ACEmanager: Events Reporting > Action Type > Type, Length, Value

- Turn-Off Services — This setting limits services and is primarily used in conjunction with monitoring data usage. For example, you could set the AirLink device to limit network service when data usage exceeds a configured threshold.

Figure 10-12: ACEmanager: Events > Actions > Action Type > Turn off Services

Email/SMS

- **To** — The email address where the report should be sent.
- **Subject** — The subject that should be displayed.
- **Message** — The message you want included with each report.
- **Body Type** — Select message in ASCI Text, SVS SCI and XML.
- **Test report** — Use to send a test report. After you have updated all the fields and clicked the Apply button, wait about 1 minute, and then click the Test report button.

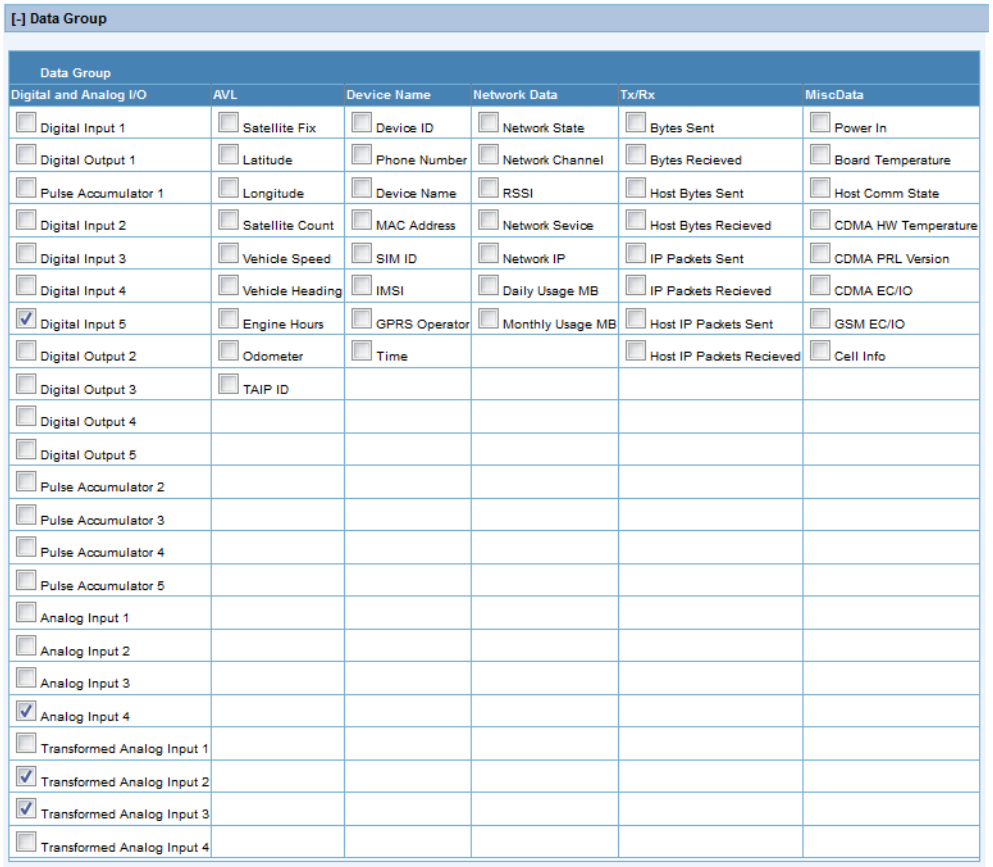
Note: You cannot send an Email with your AirLink device unless the Email server you have configured allows your AirLink device as a relay host. Talk to your network administrator to ensure you can send email through the email server using your AirLink device.

Note: You can only send SMS from your AirLink device if your cellular account allows SMS. You may need to have SMS added to the account. SMS from data accounts is blocked on some cellular networks.

Report Groups

You can select the data you want to be included in the report groups. The options are displayed. Check the box corresponding to the data displayed.

By default, all the boxes are clear.



[-] Data Group

Data Group					
Digital and Analog I/O	AVL	Device Name	Network Data	Tx/Rx	MiscData
☐ Digital Input 1	☐ Satellite Fix	☐ Device ID	☐ Network State	☐ Bytes Sent	☐ Power In
☐ Digital Output 1	☐ Latitude	☐ Phone Number	☐ Network Channel	☐ Bytes Recieved	☐ Board Temperature
☐ Pulse Accumulator 1	☐ Longitude	☐ Device Name	☐ RSSI	☐ Host Bytes Sent	☐ Host Comm State
☐ Digital Input 2	☐ Satellite Count	☐ MAC Address	☐ Network Sevice	☐ Host Bytes Recieved	☐ CDMA HW Temperature
☐ Digital Input 3	☐ Vehicle Speed	☐ SIM ID	☐ Network IP	☐ IP Packets Sent	☐ CDMA PRL Version
☐ Digital Input 4	☐ Vehicle Heading	☐ IMSI	☐ Daily Usage MB	☐ IP Packets Recieved	☐ CDMA EC/IO
☑ Digital Input 5	☐ Engine Hours	☐ GPRS Operator	☐ Monthly Usage MB	☐ Host IP Packets Sent	☐ GSM EC/IO
☐ Digital Output 2	☐ Odometer	☐ Time		☐ Host IP Packets Recieved	☐ Cell Info
☐ Digital Output 3	☐ TAIP ID				
☐ Digital Output 4					
☐ Digital Output 5					
☐ Pulse Accumulator 2					
☐ Pulse Accumulator 3					
☐ Pulse Accumulator 4					
☐ Pulse Accumulator 5					
☐ Analog Input 1					
☐ Analog Input 2					
☐ Analog Input 3					
☑ Analog Input 4					
☐ Transformed Analog Input 1					
☑ Transformed Analog Input 2					
☑ Transformed Analog Input 3					
☐ Transformed Analog Input 4					

Figure 10-13: ACEmanager: Events Reporting > Action (for GX Series device with an I/O X-Card installed)

The reports attributes are:

- Digital and Analog I/O

  The options available in this section depend on the AirLink device, and in the case of the AirLink GX Series device, whether or not it has an I/O X-Card installed.
  - Enable for Digital Inputs 1–5—The status of the specific digital inputs
  - Enable for Digital Outputs 1–5—The status of the specific digital outputs
  - Enable for Pulse Accumulator 1–5—The pulse count of the specific digital inputs
  - Enable for Analog Inputs 1–5— The status of the specific analog input (reported in volts)
  - Enable for Transformed Analog Inputs 1–5— The status of the specific analog input (reported in units configured in ACEmanager I/O > Configuration—see Configuration on page 257)
- AVL
  - Enable for Satellite Fix—Whether or not there is a usable GPS satellite fix
  - Enable for Latitude—The latitude reported by GPS
  - Enable for Longitude—The longitude reported by GPS

- Enable for Satellite Count—The number of satellites the GPS is using to get a satellite fix
- Enable for Vehicle Speed—The speed of the vehicle reported by GPS
- Enable for Vehicle Heading—The direction the vehicle is traveling reported by GPS
- Enable for Engine Hours—The number of hours the engine has been on, based on either Power In or Ignition Sense
- Enable for Odometer—The number of miles reported by GPS
- Enable for TAIP ID—The TAIP ID for the AirLink device

- Device Name

  These elements in the Device Name group are general identifiers for the AirLink device and its cellular account.
  - Enable for Device ID—The device ID (ESN or EID/IMEI) of the AirLink device (enable for a cellular account with a dynamic IP address)
  - Enable for Phone Number—The phone number of the AirLink device
  - Enable for Device Name—The name of the AirLink device
  - Enable for MAC Address—The MAC Address of the Ethernet port of the AirLink device
  - Enable for SIM ID—The SIM ID of the AirLink device
  - Enable for IMSI—The IMSI of the SIM installed in the AirLink device
  - Enable for GPRS Operator—The wireless Mobile Network Operator the SIM card is associated with
  - Enable for Time—The time the AirLink device is active
- Network Data

  The Network Data in this group relates to the cellular network and the connection state of the AirLink device.
  - Enable for Network State—The network state for the AirLink device
  - Enable for Network Channel—The network channel to which the AirLink device is connected
  - Enable for RSSI—The signal strength for the AirLink device
  - Enable for Network Service—The network service for the AirLink device
  - Enable for Network IP—The IP address given by the cellular network
  - Enable for Daily Usage MB—The daily usage (in MBs) of the AirLink device
  - Enable for Monthly Usage MB—The monthly usage (in MBs) of the AirLink device
- Tx/Rx

  The Network Traffic in this group relates to the cellular network and the network between the AirLink device and any directly connected device(s).
  - Enable for Bytes Sent—The number of bytes sent on the cellular network since last reset
  - Enable for Bytes Received—The number of bytes received from the cellular network since last reset
  - Enable for Host Bytes Sent—The number of bytes sent from the network between the AirLink device and the connected device(s) since last reset
  - Enable for Host Bytes Received—The number of bytes received from the network between the AirLink device and the connected device(s) since last reset
  - Enable for IP Packets Sent—The number of IP packets sent on the cellular network since last reset

  - Enable for IP Packets Received—The number of IP packets received from the cellular network since last reset
  - Enable for Host IP Packets Sent—The number of IP packets sent from the network between the AirLink device and the connected device(s) since last reset
  - Enable for Host IP Packets Received—The number of IP packets received from the network between the AirLink device and the connected device(s) since last reset
- Misc Data

  Miscellaneous Data includes temperature rates and other information that does not fit in the other categories
  - Enable for Power In—The voltage level of the power coming in to the AirLink device at the time of the report
  - Enable for Board Temperature—The temperature of the internal hardware of the AirLink device at the time of the report
  - Enable for Host Comm State—The signal level between the AirLink device and the connected device(s)
  - CDMA HW Temperature—The temperature of the internal radio module
  - CDMA PRL Version—PRL version used by the AirLink device
  - CDMA EC/IO—The quality of the signal from the cellular CDMA network
  - GSM EC/IO—The quality of the signal from the cellular GSM network
  - Cell Info—The cellular network cell information for the AirLink device

Note: For each group you can enable individual fields.

Relay

The relay outputs on the AirLink device I/O port can be used to cause an external action.

- 1—Relay 1—Open
- 2—Relay 1, Inverted—Closed

The relays are capable of switching small loads. If you need a stronger signal, such as to open a door lock, connect the AirLink device's relay to a stronger solenoid relay that has enough power to cause the desired effect.

Configure Events

To configure events,

1. Enter an Event Description. The event description will be displayed in the Events group in the left hand side panel.
2. Select any action and click Add Action. Then select any Action Type and configure accordingly.
3. Click Save and the action will be displayed in the Available Actions menu.

Events Protocol

The Events Reporting protocol is a collection of messaging formats. The messages are sent to the Reports Server.

The Events Protocol includes four message types.

- **1 — Type, Length, Value** — The TLV consists of the MSCI ID as the type, the length of the data, and the actual data.
- **2 — Binary** — A binary condensed form of the TLV message will be sent.
- **3 — CSV-ASCII** — An ASCII condensed and comma delimited form of the TLV message will be sent.
- **4 — XML** — An XML form of the data will be sent.

Tip: *Because of its flexibility and robustness, the TLV message type is recommended for most reports using the Events Protocol. The Binary and ASCII forms do not contain a "type field" which can result in misinterpretation of data. Since the TLV and XML forms always includes the type as well as the data, an unintentional type can be identified much easier.*

11: Serial Configuration

11

Use the serial port to connect devices or computers using a DB9-RS232 connection.

Note: These commands are specific to the RS232 port and generally do not apply to USB/serial.

Port Configuration

Serial Port Configuration consists of five categories of configurable parameters:

- Port Configuration
- Advanced
- TCP
- UDP
- PPP

These categories and their parameters are shown in Figure 11-1, Figure 11-2, and Figure 11-3 and described in Table 11-1, Table 11-2, and Table 11-3.

Port Configuration

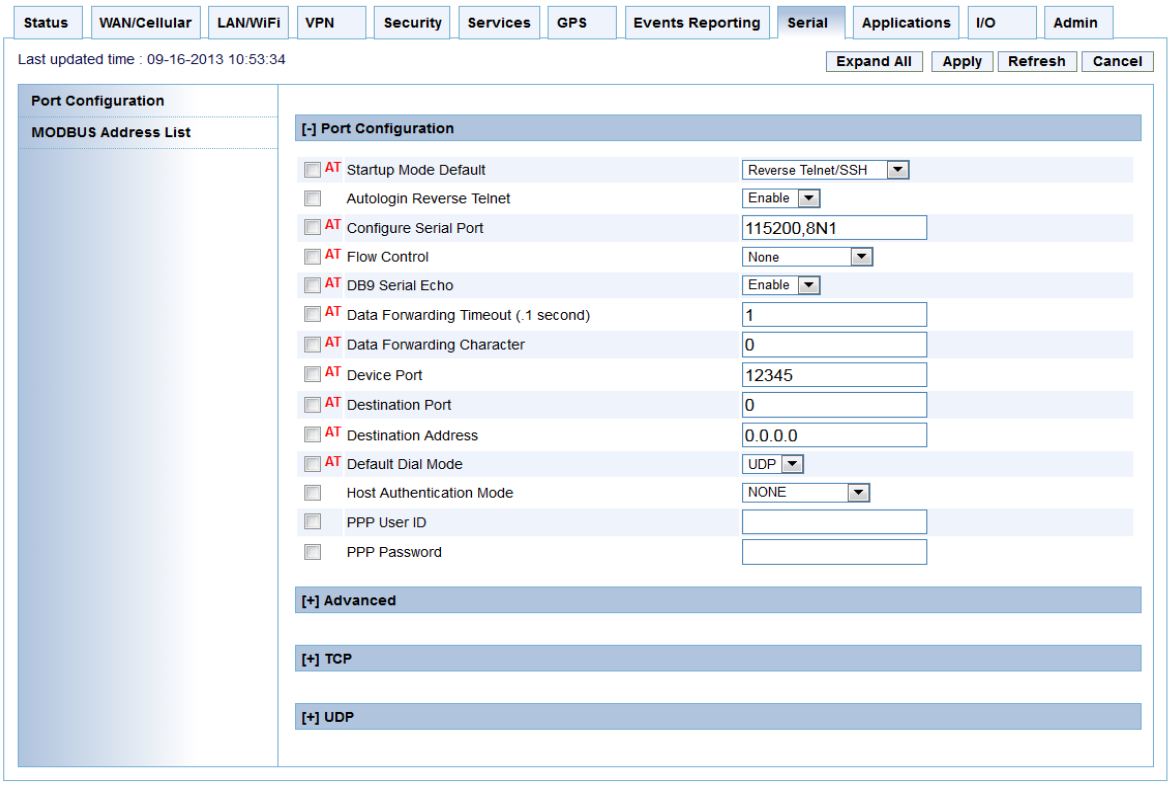


Figure 11-1: ACEmanager: Serial > Port Configuration > Port Configuration

Table 11-1: Serial Port Configuration > Port Configuration

Field	Description
Port Configuration	
Startup Mode Default	Default power-up mode for the serial port. When the AirLink device is power-cycled, the serial port enters the communication mode specified. *Note: It can take up to 5 minutes to establish a connection.* • Normal (AT command) default • PPP • UDP • TCP • Reverse Telnet/SSH—Allows you to telnet or SSH into a router or other device connected to the AirLink device via a serial port. For information on configuring reverse telnet, see Reverse Telnet/SSH on page 224. • Modbus ASCII • Modbus RTU (Binary) • BSAP—Bristol Standard Asynchronous Protocol • Variable Modbus • UDP Multiple Unicast—Data from the serial port is packed into UDP packets and sent to multiple IP addresses (for example, multiple AirLink devices). For more information, see UDP Multiple Unicast on page 227. You can also use an AT command to configure this field. See MD on page 361.
Autologin reverse telnet	This field only appears when the Startup Mode Default field is set to reverse telnet/SSH. Determines the log in procedure when using reverse telnet. • Enable—Do not enter a user name and password when you telnet to a a router or other device that has a serial connection to your AirLink device. Login is automatic. • Disable—Enter a user name and password when you telnet to a a router or other device that has a serial connection to your AirLink device. (Default) For more information about reverse telnet, see Reverse Telnet/SSH on page 224.
Configure Serial Port	Format: [speed][data bits][parity][stop bits] Valid speeds are 300–115200, data bits: 7 or 8, parity: O,E,N,M, stop bits: 1,1.5. You can also use an AT command to configure this field. See S23 on page 370.
Flow Control	Serial port flow control setting • None—No flow control is being used (default) • Hardware—RTS/CTS hardware flow control is being used • Transparent SW—Transparent software flow control. Uses escaped XON and XOFF for flow control. XON and XOFF characters in data stream are escaped with the @ character (0x40). @ in data is sent as @@. You can also use an AT command to configure this field. See \Q on page 369.
DB9 Serial Echo	AT command echo mode • Enable—Text is visible as you type (default) • Disable—Text you type is not visible You can also use an AT command to configure this field. See E on page 368.

Table 11-1: Serial Port Configuration > Port Configuration

Field	Description
Data Forwarding Timeout (.1 seconds)	Data forwarding time-out. (How long the application waits before bundling characters to send) If set to 0, a forwarding time-out of 10 ms is used. Used in UDP or TCP PAD mode. Increments in tenths of a second. Default value is 1 (The forward time-out is 100 ms) You can also use an AT command to configure this field. See S50 on page 364.
Data Forwarding Character	PAD data forwarding character. ASCII code of character that causes data to be forwarded. Used in UDP or TCP PAD mode Default is No forwarding character. You can also use an AT command to configure this field. See S51 on page 364.
Device Port	The port on the AirLink device used for incoming TCP/UDP communication (Default is 12345) If either, or both, of the UDP Auto Answer or TCP Auto Answer parameters are enabled, when the AirLink device receives incoming TCP or UDP packets that are destined for this port, it strips off the IP header and send the packet payload out its serial port. You can also use an AT command to configure this field. See *DPORT on page 360.
Destination Port	The destination port that TCP/UDP communication is sent to You can also use an AT command to configure this field. See S53 on page 364.
Destination Address	IP address TCP/UDP communication is sent to You can also use an AT command to configure this field. See S53 on page 364.
Default Dial Mode	Protocol used to send messages Options are: • TCP • UDP (default) You can also use an AT command to configure this field. See S53 on page 364.
Host Authentication Mode	Sets the authentication method the host uses for PPP. Options are: • None • CHAP—The stronger of the two protocols. Recommended, provided it is supported by all the client devices • PAP and CHAP—If CHAP is not supported by the client, the host reverts to PAP.
PPP User ID	Sets the User ID for authentication
PPP Password	Sets the User Password for authentication

For information on configuring an AirLink device to use SSH PAD mode, see SSH PAD Mode on page 22.

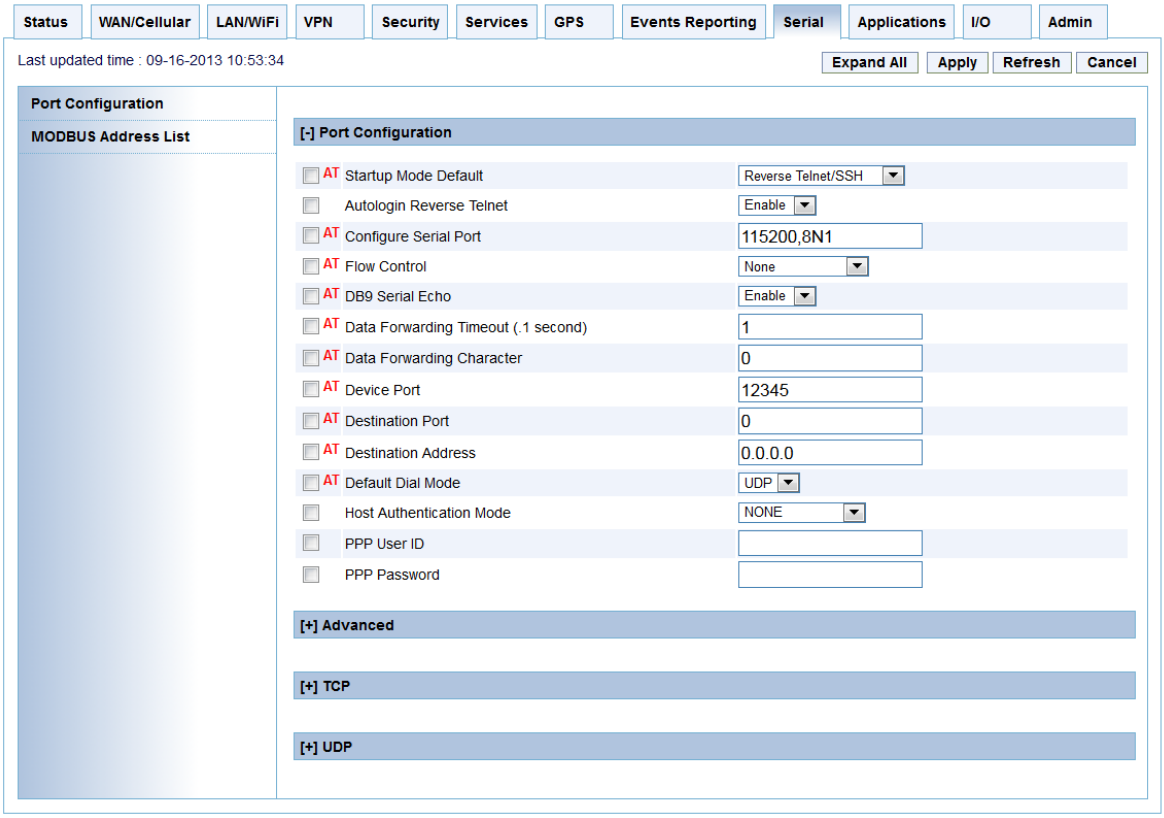
Reverse Telnet/SSH

The Reverse Telnet/SSH feature allows you to connect to and configure a router or other device that has a serial connection to your AirLink device.

Note: If you have all 5 VPN tunnels configured, you cannot use Reverse Telnet/SSH.

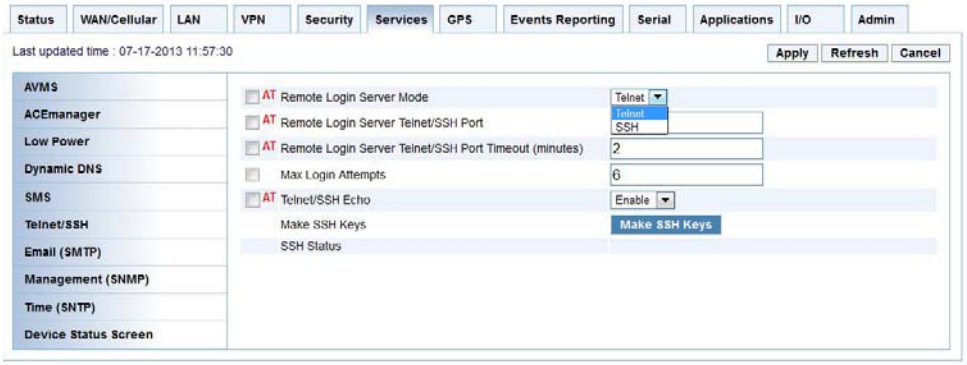
To configure Reverse Telnet/SSH:

1. Log into ACEmanager and go to Serial > Port Configuration.
2. In the Startup Mode Default field, select Reverse Telnet/SSH and click Apply.
3. In the Configure Serial Port field, set the speed, data bits, parity, and stop bits. (The serial port configuration depends on the router you want to connect to. For example, to connect to a Cisco router that has a default baud rate of 9600, enter 9600,8N1 in the Configure Serial Port field.)

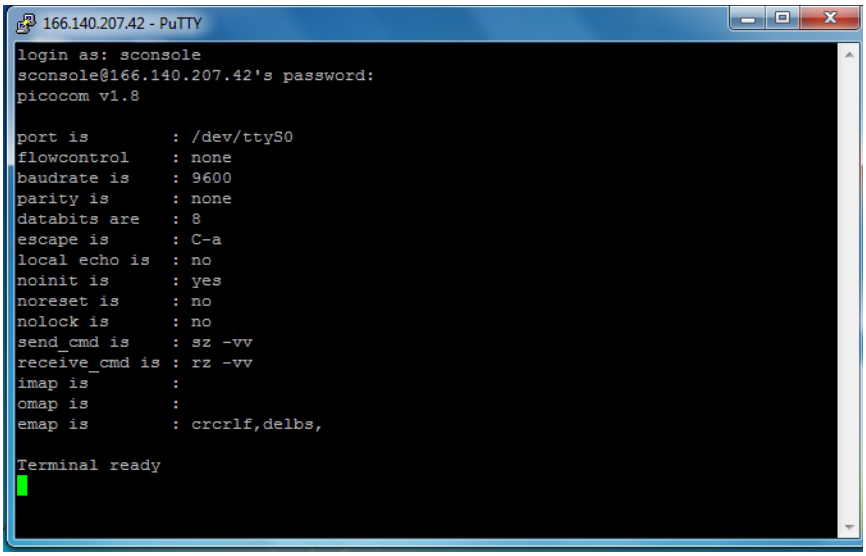


4. Optional—If you are planning to use telnet (rather than SSH), you can be automatically logged in when you telnet to the AirLink device without having to enter a user name and password. Autologin is not supported with SSH. To set up automatic login:
   a. In the Autologin Reverse Telnet field, select Enable.
   b. Click Apply.
5. Go to Services > Telnet/SSH.
6. In the Remote Login Server Mode field, select:
   - Telnet—if you want to Telnet into the connected device
   - SSH—if you want to SSH into the connected device

Note: If you enabled Autologin, select Telnet.



7. Click Apply.
8. Reboot the AirLink device.
9. Use a Telnet or SSH terminal client such as Putty or Teraterm to connect to the appropriate port:
   - If you are using Autologin, Telnet to the port specified in the Device Port field (default is 12345). SSH is not available with Autologin.
   - If you are not using Autologin, you can Telnet or SSH into the port specified in the Remote Login Server Telnet/SSH Port field (default is 2332).
10. If prompted, log in with the following credentials:
    - User name: sconsole
    - Password: 12345 (default)



For information on changing the default reverse telnet password, see Change Password on page 261.

ALEOS redirects you to the router or other device connected to the AirLink device serial port. You can use this connection to configure connected device.

Note: You may be required to enter a user name and password to access the router or other device.

UDP Multiple Unicast

With UDP Multiple Unicast, data from the serial port is packed into UDP packets and sent to multiple IP addresses. To configure UDP Multiple Unicast:

1. Log in to ACEmanager as “user” and go to Serial > Port Configuration > Port Configuration.
2. In the Startup Mode Default field, select UDP Multiple Unicast.
3. In the Destination Port field, enter the remote port to be used.
4. Click Apply.
5. Go to Serial > Modbus Address List and enter the index numbers and IP addresses of the devices you want the data sent to. (See Modbus Address List on page 234.)
6. Click Apply.
7. Reboot the device.

Note: To avoid flooding the network, there is a 20 millisecond pause between sending the UDP packet to each destination.

Advanced

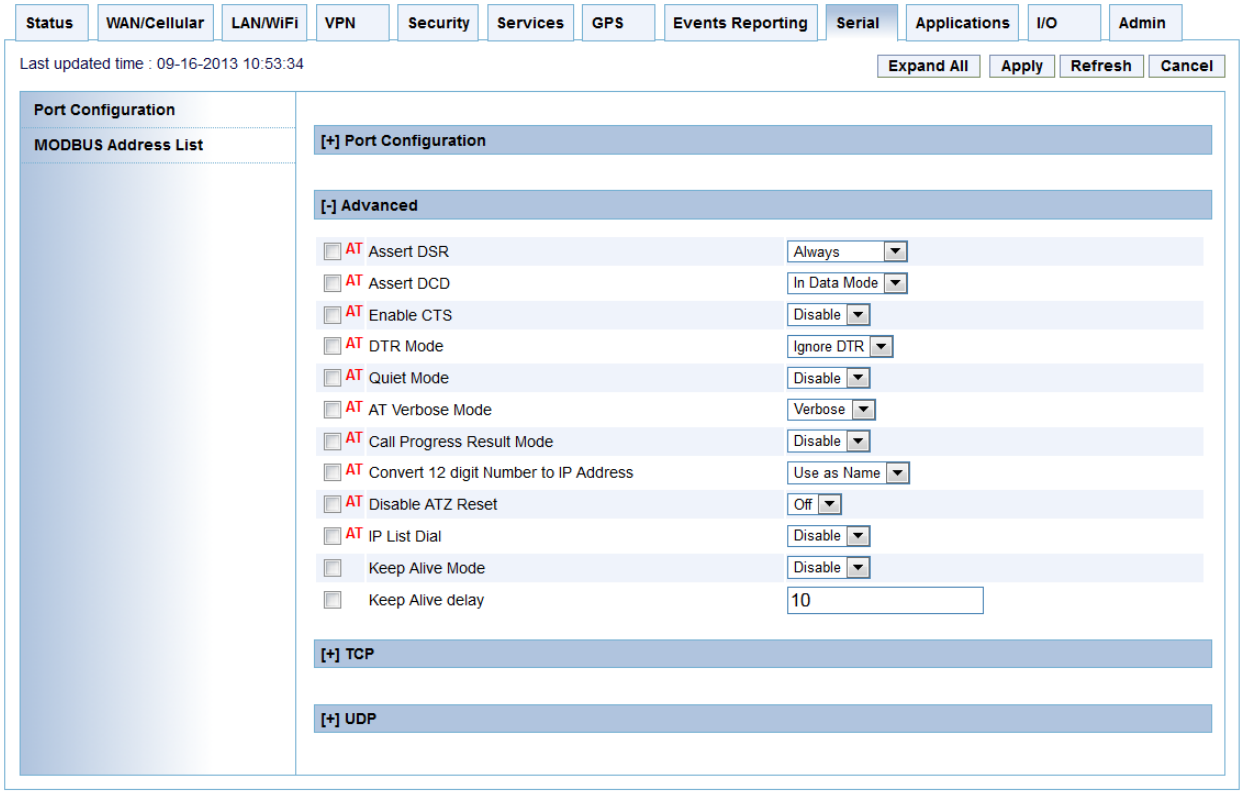


Figure 11-2: ACEmanager: Serial > Port Configuration > Advanced

Table 11-2: Serial Port Configuration > Advanced

Field	Description
Advanced	
Assert DSR	Assert DSR always when the device is in a data mode (UDP, TCP, etc.), or when the device is in network coverage. Options are: • Always (default) • In Data Mode • In Coverage You can also use an AT command to configure this field. See &S on page 369.
Assert DCD	Assert DCD always, or when the device is in a data mode (UDP, TCP, etc.) or when the device is in network coverage. Options are: • Always (default) • In Data Mode • In Coverage You can also use an AT command to configure this field. See &C on page 366.

Table 11-2: Serial Port Configuration > Advanced

Field	Description
Enable CTS	Assert CTS when there is network coverage. Options are: • Disable (default) • Enable You can also use an AT command to configure this field. See *CTSE on page 360.
DTR Mode	Use DTR from the serial device, or ignore DTR (same as S211 on page 370). Options are: • Use DTR • Ignore DTR (default)
Quiet Mode	Disable or enable display of device responses. Options are: • Disable (default) • Enable You can also use an AT command to configure this field. See Q on page 368.
AT Verbose Mode	Sets the level of information returned for AT commands Options are: • Verbose (default) • Numeric You can also use an AT command to configure this field. See V on page 371.
Call Progress Result Mode	When enabled adds 19200 to CONNECT messages Options are: • Disable (default) • Enable You can also use an AT command to configure this field. See X on page 371.
Convert 12 digit Number to IP Address	Choose whether a 12-digit number is converted to an IP address (eg. 111222333444 to 111.222.333.444). Options are: • Use as Name (default) • Use as IP You can also use an AT command to configure this field. See *NUMTOIP on page 363
Disable ATZ Reset	The value set in this field determines whether or not issuing an ATZ Command resets the AirLink device. Options are: • On — Block is enabled—ATZ does not reset the device. • Off —Block is disabled—ATZ resets the device. (default) You can also use an AT command to configure this field. See *DATZ on page 368.
IP List Dial	This allows access to the Modbus IP Address using the first two digits of the dial string. For example, ATDT1234567 would imply ID index 12 on the Modbus Address list and use the associated IP Address as the destination. Options are: • Disable (default) • Enable You can also use an AT command to configure this field. See IPL on page 363.

Table 11-2: Serial Port Configuration > Advanced

Field	Description
Keep Alive Mode	When this feature is enabled, the AirLink device reboots if there is no traffic for longer than the period configured in the Keep Alive Delay field. Options are” • Disable (default) • Enable
Keep Alive Delay	When Keep Alive Mode is enabled, use this field to set the delay (in minutes) before the AirLink device reboots if there is no traffic on the serial port. Accepted values: • 10–65535

TCP

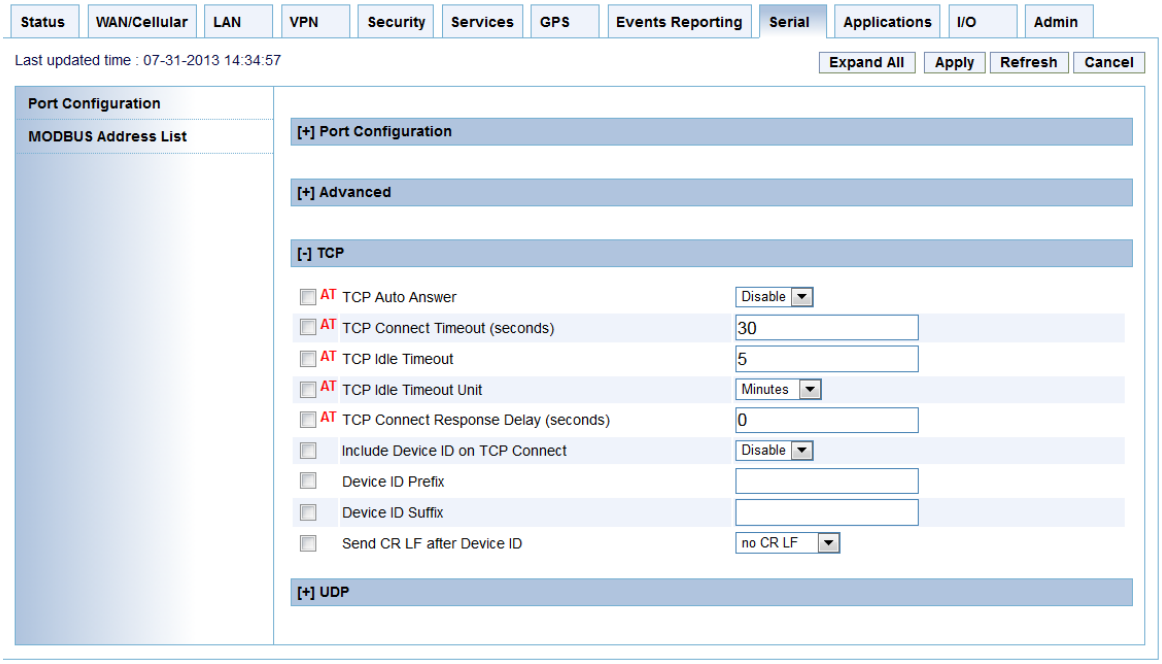


Figure 11-3: ACEmanager: Serial > Port Configuration > TCP

Table 11-3: Serial Port Configuration > TCP

Field	Description
TCP	
TCP Auto Answer	This determines how the AirLink device responds to an incoming TCP connection request. The AirLink device remains in AT Command mode until a connection request is received. The AirLink device sends a “RING” string to the host. A “CONNECT” sent to the host indicates acknowledgment of the connection request and the TCP session is established. • Disable (default) • Enable You can also use an AT command to configure this field. See S0 on page 369.

Table 11-3: Serial Port Configuration > TCP

Field	Description
TCP Connect Timeout (seconds)	Specifies the number of seconds to wait for a TCP connection to be established when dialing out You can also use an AT command to configure this field.
TCP Idle Timeout	TCP idle time-out in the configured units (See TCP Idle Timeout Unit on page 231.) Specifies a time interval upon which if there is no in or outbound traffic through a TCP connection, the connection is terminated. Default is 0. You can also use an AT command to configure this field. See TCPT on page 365.
TCP Idle Timeout Unit	Units used for the TCP Idle Timeout Interval. Options are: • Minutes (default) • secs You can also use an AT command to configure this field. See TCPS on page 365.
TCP Connect Response Delay (seconds)	The number of seconds to delay the “CONNECT' response upon establishing a TCP connection, or the number of tenths of seconds to delay before outputting ENQ on the serial port after the CONNECT when the ENQ feature is enabled. • n=0–255 You can also use an AT command to configure this field. See S221 on page 370.
Include Device ID on TCP Connect	If this option is enabled, after a TCP connection is established, ALEOS sends a packet that contains the device ID (and optionally a prefix, suffix, and CRLF). Options are: • Disable (default) • Enable *Note: To use this feature, ensure that the Device ID is configured in the Use Device ID in Location Reports field on the GPS screen (GPS > Global Settings > General). See Global Settings on page 204.*
Device ID Prefix	Sets the Prefix DID in the device identification packet upon TCP connection. Maximum length of the prefix is 80 characters.
Device ID Suffix	Sets the Suffix DID in the device identification packet upon TCP connection. Maximum length of the suffix is 80 characters.
Send CR LF after Device ID	Enables a carriage return to be inserted in the device identification packet after the Suffix DID. Options are: • no CR LF • send CR • send CR LF (carriage return, line feed) Default

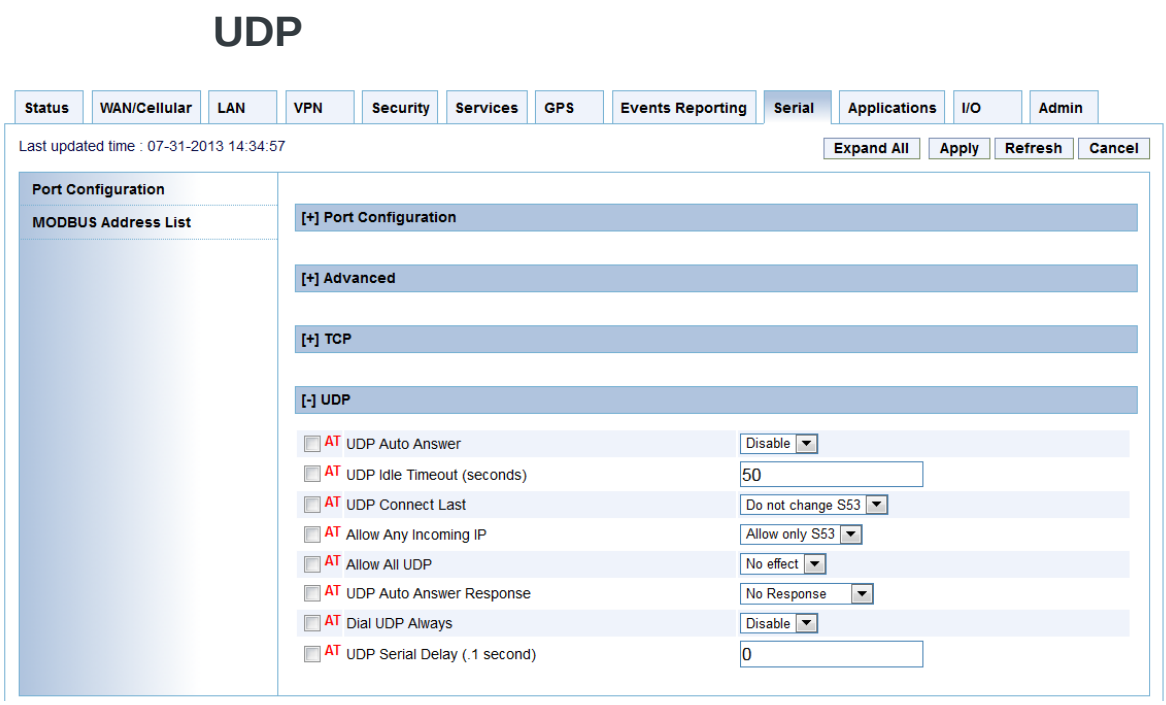


Figure 11-4: ACEmanager: Serial > Port Configuration > UDP

Table 11-4: Serial Port Configuration > UDP

Field	Description
UDP	
UDP Auto Answer	Whether the AirLink device auto answers and incoming UDP connection request Options are: • Disable (default) • Enable You can also use an AT command to configure this field. See S82 on page 364.
UDP Idle Timeout (seconds)	UDP Idle Time-out in seconds Specifies a time interval upon which if there is no in or outbound traffic through a UDP connection, the connection is terminated. • n=0 No idle time-out (Default) • n=1–255 Time-out in seconds You can also use an AT command to configure this field. See S83 on page 365.
UDP Connect Last	Allows you to choose to use the last accepted IP address and port number as the default settings, instead of using S53 (destination address) Options are: • Do not change S53 (default) • Set S53 last IP *Note: Resetting the device restores the configured S53 (destination address).* You can also use an AT command to configure this field. See *UDPLAST on page 365.

Table 11-4: Serial Port Configuration > UDP

Field	Description
Allow Any Incoming IP	When UDP auto answer is enabled, use this field to select whether to allow any incoming IP address to connect or to only allow the configured destination IP address to connect. Options are: • Allow only S53 (default) • Allow any IP address If you select Allow only S53, the Destination Port and Destination Address fields under Serial > Port Configuration must be configured. (See Table 11-1 on page 223.) You can also use an AT command to configure this field. See AIP on page 360.
Allow All UDP	Accepts UDP packets from all IP addresses when a UDP session is active. If there is no UDP session active, an incoming UDP packet is treated according to the UDP auto answer and AIP settings. Options are: • No effect (default) • Allow all—The AirLink device accepts all UDP traffic from any IP address during a UDP session. You can also use an AT command to configure this field. See *UALL on page 365.
UDP Auto Answer Response	Half-Open Response—In UDP auto answer (half-open) mode. Options are: • No Response—No Response codes when UDP session is initiated (default) • RING CONNECT—RING CONNECT response codes sent out serial link before the data from the first UDP packet *Note: Quiet Mode must be Off.* You can also use an AT command to configure this field. See HOR on page 368.
Dial UDP Always	The dial command always uses UDP, even when using ATDT. Options are: • Disable—Dial using the means specified (default) • Enable—Dial UDP always, even when using ATDT *Note: When this parameter is set you cannot establish a TCP PAD connection.* You can also use an AT command to configure this field. See *DU on page 361.
UDP Serial Delay (.1 seconds)	Waits the specified delay before sending the first received UDP packet and the subsequent UDP packets out to the port Ethernet (in 100 ms units). • No UDP packet delay (default) • 1–255— Delay in 100ms units, from 100 ms to 25.5 sec. You can also use an AT command to configure this field. See *USD on page 365.

PPP

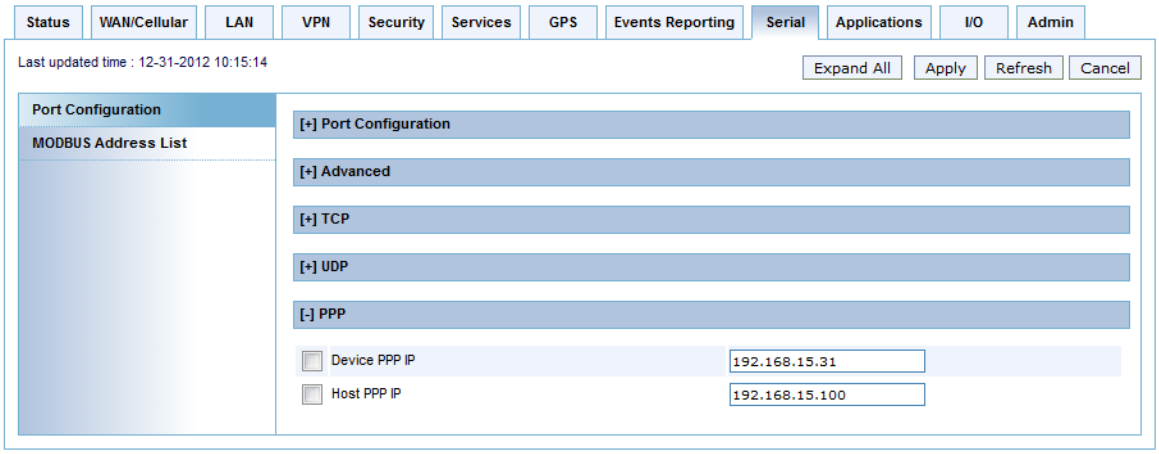


Figure 11-5: ACEmanager: Serial > Port Configuration > PPP

Table 11-5: Serial Port Configuration > PPP

Field	Description
PPP[a]	
Device PPP IP	Sets the device IP address (in private mode)
Host PPP IP	Sets the host IP address (in private mode)

a. Note: This section is only visible when PPP is selected in the Startup Mode Default field.

Modbus Address List

To add a Modbus Address:

1. Log in to ACEmanager as “user” and go to Serial > MODBUS Address List.
2. Click Add More.
3. Enter the Index number, an equal sign, and the IP address. For example:
   10=123.123.123.123 (decimal)

   0xA=123.123.123.123 (hex) Prefix 0x to hex numbers.

   Including the port number after the IP address is optional. If you include the port number, separate the port number and IP address by a colon.
   For example:

   10=123.123.123.123:11223

   0xA=123.123.123.123:11223

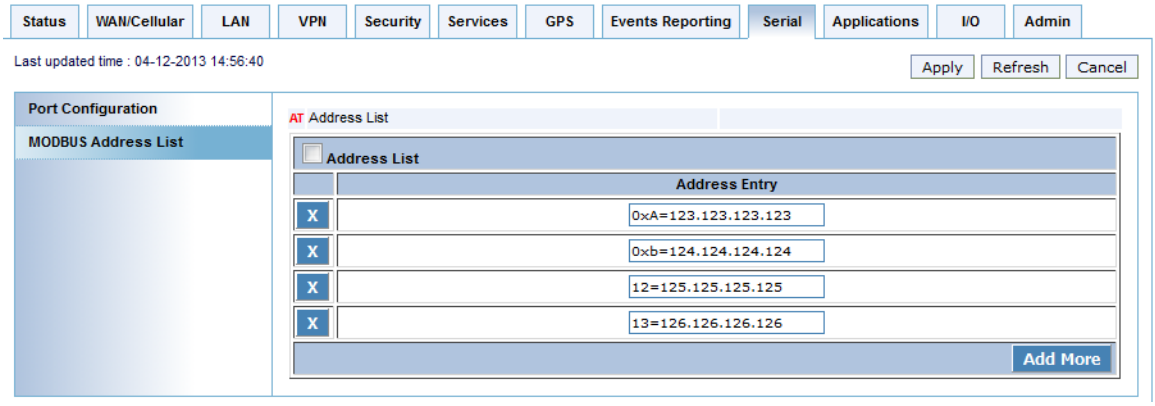


Figure 11-6: Serial > MODBUS Address List

4. Click Apply.
5. Reboot.

To delete an address from the list, click the X beside it.

Note: You can also use the AT Commands MLIST and MLISTX to add address entries and MLIST? or MLISTX? to query the entries on the list. See MLIST on page 362, and MLISTX on page 362.

I/O X-Card Serial Port Configuration

This section applies only to the AirLink GX Series device with an I/O X-Card installed. The serial port on the I/O X-Card is a standard RS232 port using five wires: RX, TX, RTS, CTS, and GND. The following are not supported: RI, DCD, DTR, and DSR. For more information on the I/O X-Card, refer to the AirLink GX Series User Guide.

To configure the serial port for the installed I/O X-Card:

1. In ACEmanager, go to Serial > I/O X-Card Serial Port.

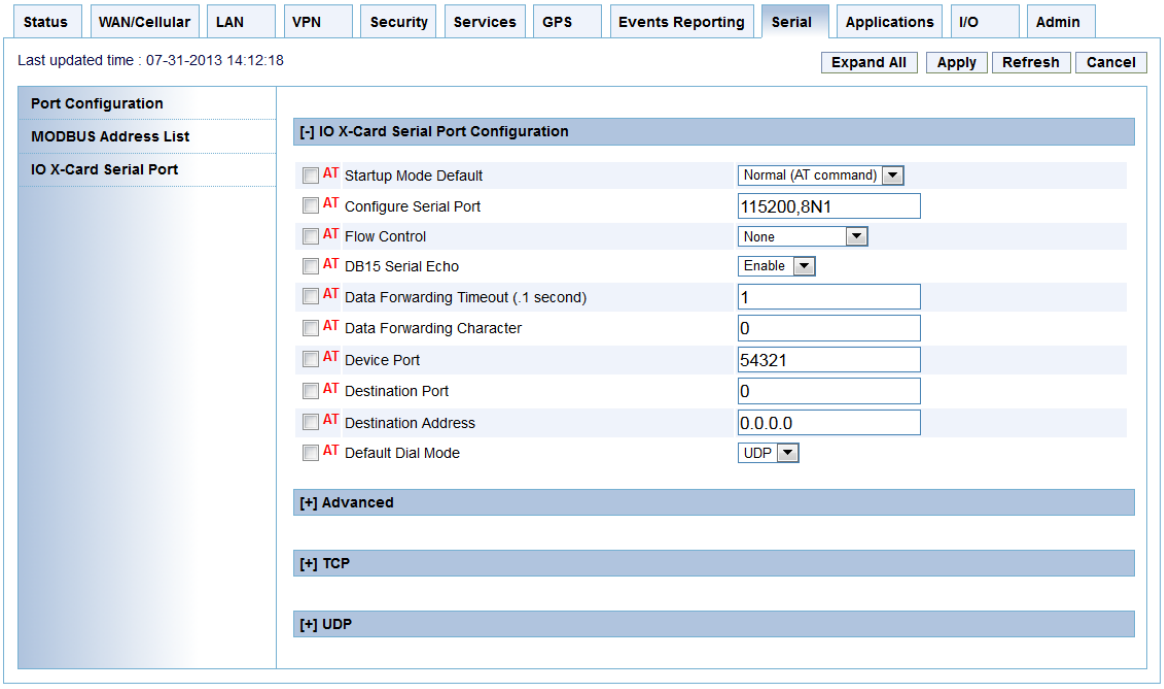


Figure 11-7: ACEmanager: Serial > IO X-Card Serial Port > IO X-Card Serial Configuration

Table 11-6: Serial > IO X-Card Serial Port > IO X-Card Serial Configuration

Field	Description
Startup Mode Default	The default startup mode for the serial port Options are: • Normal (AT command) default • UDP • TCP You can also use an AT command to configure this field. See MD on page 361.
Configure Serial Port	Format: [speed],[data bits][parity][stop bits] Valid speeds are 300–115200, data bits: 7 or 8, parity: O,E,N,M, stop bits: 1,1.5,2 • 115200, 8N1 (default) You can also use an AT command to configure this field. See S23 on page 370.
Flow Control	Serial port data flow control setting • None—No flow control is being used (default) • Hardware—RTS/CTS hardware flow control is being used • Transparent SW—Transparent software flow control. Uses escaped XON and XOFF for flow control. XON and XOFF characters in data stream are escaped with the @ character (0x40). @ in data is sent as @@. You can also use an AT command to configure this field. See \Q on page 369.

Table 11-6: Serial > IO X-Card Serial Port > IO X-Card Serial Configuration

Field	Description
DB15 Serial Echo	AT command echo mode Options are: • Enable—Text is visible as you type. (default) • Disable—Text you type is not visible. You can also use an AT command to configure this field. See E on page 368.
Data Forwarding Timeout (.1 second)	Data forwarding time-out. (How long the application waits before bundling characters to send) If set to 0, a forwarding time-out of 10ms is used. Used in UDP or TCP PAD mode. Increments in tenths of a second. Default is 1 (The forwarding time-out is 100 ms.) You can also use an AT command to configure this field. See S50 on page 364.
Data Forwarding Character	PAD data forwarding character. ASCII code of character that causes data to be forwarded. Used in UDP or TCP PAD mode Default is No forwarding character You can also use an AT command to configure this field. See S51 on page 364.
Device Port	The port on the AirLink device used for incoming TCP/UDP communication (Default is 54321) If either, or both, of the UDP Auto Answer or TCP Auto Answer parameters are enabled, when the AirLink device receives incoming TCP or UDP packets that are destined for this port, it strips off the IP header and send the packet payload out the serial port on the I/O X-Card. You can also use an AT command to configure this field. See *DPORT on page 360.
Destination Port	The destination port that TCP/UDP communication is sent to You can also use an AT command to configure this field. See S53 on page 364.
Destination Address	The IP address TCP/UDP communication is sent to You can also use an AT command to configure this field. See S53 on page 364.
Default Dial Mode	Protocol used to send messages Options are: • TCP • UDP (default) You can also use an AT command to configure this field. See S53 on page 364.

Advanced Settings

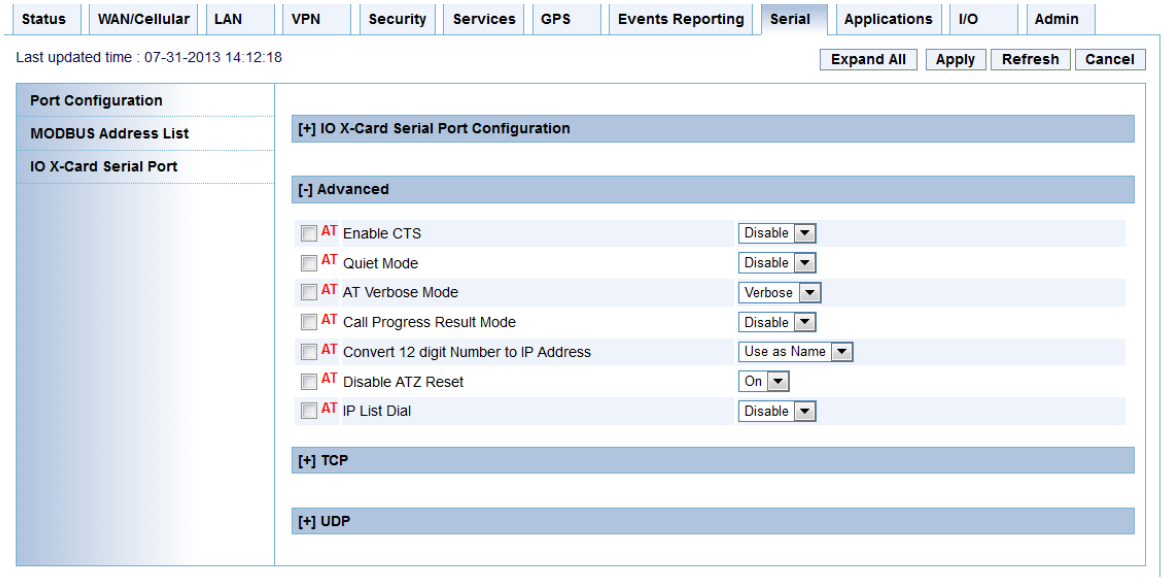


Figure 11-8: ACEmanager: Serial > IO X-Card Serial Port > Advanced

Table 11-7: Serial > X-Serial Port Configuration >Advanced and TCP Configuration

Field	Description
Enable CTS	Assert CTS when there is network coverage. Options are: • Disable (default) • Enable You can also use an AT command to configure this field. See *CTSE on page 360.
Quiet Mode	Disable or enable display of device responses. Options are: • Enable • Disable (default) You can also use an AT command to configure this field. See Q on page 368.
AT Verbose Mode	Sets the level of information returned for AT commands Options are: • Verbose (default) • Numeric You can also use an AT command to configure this field. See V on page 371.
Call Progress Result Mode	When enabled adds 19200 to CONNECT messages. Options are: • Enable • Disable (default) You can also use an AT command to configure this field. See X on page 371.

Table 11-7: Serial > X-Serial Port Configuration >Advanced and TCP Configuration

Field	Description
Convert 12 digit Number to IP Address	Choose whether or not a 12-digit number is converted to an IP address For example, converts 111222333444 to 111.222.333.444 Options are: • Use as Name (default) • Use as IP You can also use an AT command to configure this field. See *NUMTOIP on page 363.
Disable ATZ Reset	The value set in this field determines whether or not issuing an ATZ Command resets the AirLink device. Options are: • On (default) — ATZ does not reset the AirLink device • Off —ATZ resets the AirLink device. You can also use an AT command to configure this field. See *DATZ on page 368.
IP List Dial	This allows access to the Modbus IP Address using the first two digits of the dial string. For example, ATDT1234567 would imply ID index 12 on the Modbus Address list and use the associated IP Address as the destination. Options are: • Enable • Disable (default) You can also use an AT command to configure this field. See IPL on page 363.

TCP Settings

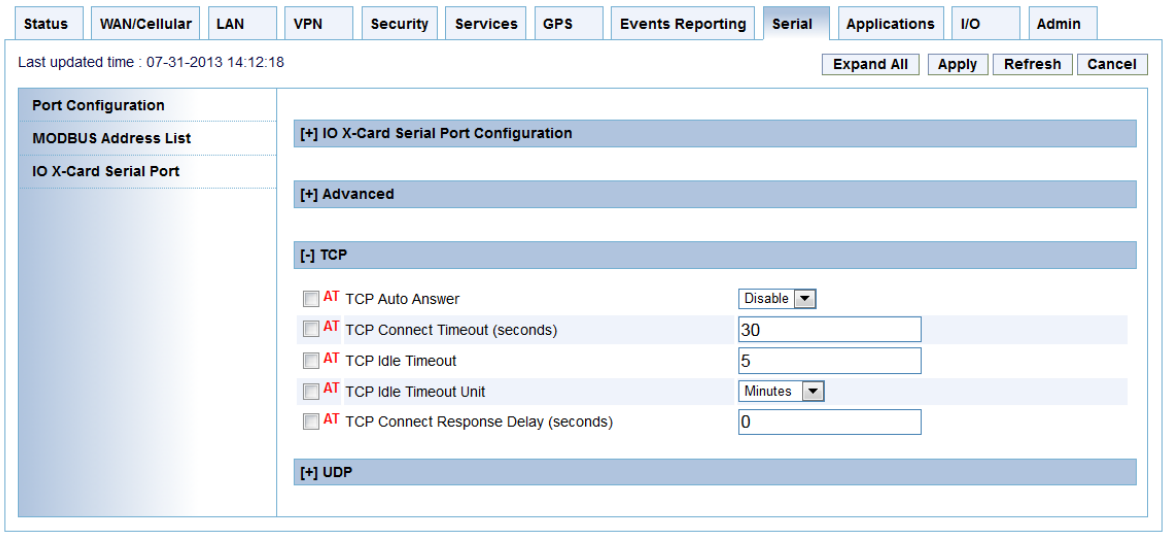


Figure 11-9: ACEmanager: Serial > IO X-Card Serial Port > TCP

Table 11-8: Serial > X-Serial Port Configuration >Advanced and TCP Configuration

Field	Description
TCP Auto Answer	This determines how the AirLink device responds to an incoming TCP connection request. The AirLink device remains in AT Command mode until a connection request is received. The AirLink device sends a “RING” string to the host. A “CONNECT” sent to the host indicates acknowledgment of the connection request and the TCP session is established. Options are: • Enable • Disable (default) You can also use an AT command to configure this field. See S0 on page 369.
TCP Connect Timeout (seconds)	Specifies the number of seconds to wait for a TCP connection to be established when dialing out You can also use an AT command to configure this field.
TCP Idle Timeout	TCP idle time-out in the configured units (See TCP Idle Timeout Unit on page 231.) Specifies a time interval upon which if there is no in or outbound traffic through a TCP connection, the connection is terminated. Default is 0. You can also use an AT command to configure this field. See TCPT on page 365.
TCP Idle Timeout Unit	Units used for the TCP Idle Timeout interval Options are: • Minutes (default) • secs You can also use an AT command to configure this field. See TCPS on page 365.
TCP Connect Response Delay (seconds)	The number of seconds to delay the “CONNECT' response upon establishing a TCP connection, or the number of tenths of seconds to delay before outputting ENQ on the serial port after the CONNECT when the ENQ feature is enabled. • n=0–255 You can also use an AT command to configure this field. See S221 on page 370.

UDP Settings

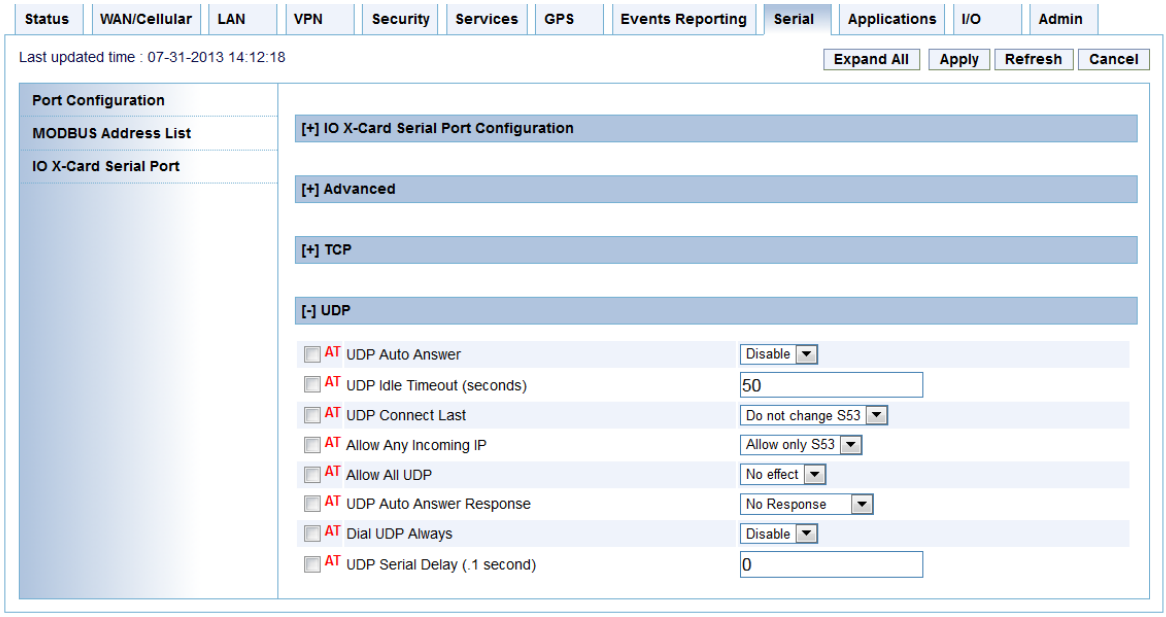


Figure 11-10: ACEmanager: Serial > IO X-Card Serial Port > UDP

Table 11-9: Serial > IO X-Card Serial Port > UDP

Field	Description
UDP Auto Answer	Whether the AirLink device auto answers an incoming UDP connection request Options are: • Enable • Disable (default) You can also use an AT command to configure this field. See S82 on page 364.
UDP Idle Timeout (seconds)	UDP idle time-out in seconds Specifies a time interval upon which if there is no in or outbound traffic through a UDP connection, the connection is terminated. You can also use an AT command to configure this field. See S83 on page 365.
UDP Connect Last	Allows you to choose to use the last accepted IP address and port number as the default settings, instead of using S53 (destination address) Options are: • Do not change S53 — Does not change the destination IP address (default) • Set S53 as last —Uses the last accepted IP address *Note: Resetting the device restores the configured S53 (destination address).* You can also use an AT command to configure this field. See *UDPLAST on page 365.

Table 11-9: Serial > IO X-Card Serial Port > UDP

Field	Description
Allow Any Incoming IP	When UDP auto answer is enabled, use this field to select whether to allow any incoming IP address to connect or to only allow the configured destination IP address to connect. Options are: • Allow only S53 —Allows only the configured destination IP address (default) • Allow any IP If you select Allow only S53, the Destination Port and Destination Address fields under Serial > X-Serial Port Configuration must be configured (See Table 11-6 on page 236.) You can also use an AT command to configure this field. See AIP on page 360.
Allow All UDP	Accepts UDP packets from all IP addresses when a UDP session is active. If there is no UDP session active, an incoming UDP packet is treated according to the UDP auto answer and AIP settings. Options are: • No effect (default) • Allow all—The AirLink device accepts all UDP traffic from any IP address during a UDP session You can also use an AT command to configure this field. See *UALL on page 365.
UDP Auto Answer Response	Half-Open Response—In UDP auto answer (half-open) mode. Options are: • No Response—No Response codes when UDP session is initiated (default) • RING CONNECT—RING CONNECT response codes sent out over the serial link before the data from the first UDP packet *Note: Quiet Mode must be Off.* You can also use an AT command to configure this field. See HOR on page 368.
Dial UDP Always	The dial command always uses UDP, even when using ATDT. Options are: • Disable—Dial using the means specified (default) • Enable—Dial UDP always, even when using ATDT *Note: When this parameter is set you cannot establish a TCP PAD connection.* You can also use an AT command to configure this field. See *DU on page 361.
UDP Serial Delay (.1 seconds)	Waits the specified delay before sending the first received UDP packet and the subsequent UDP packets out to the Ethernet port (in 100 ms units). • No UDP packet delay (Default) • 1–255—Delay in 100ms units, from 100 ms to 25.5 sec. You can also use an AT command to configure this field. See *USD on page 365.

12: Application Configuration

The Applications tab consists of a Data Usage section, a Garmin application, and an ALEOS Application Framework section.

Data Usage

The Data Usage feature available in the Application tab provides you with a way to actively monitor cellular data usage.

You can:

- Actively monitor the cellular data usage by configuring usage level thresholds that result in notifications being sent to you.
- Halt device data traffic until the end of the billing period. In the event that you decide to halt the data traffic, the management interface to ALEOS is still available.
- Set usage levels and thresholds on a monthly and/or daily limit.

Note: ALEOS Data Usage is approximate and should not be compared with data usage recorded by the Mobile Network Operator.

SIERRA WIRELESS IS NOT RESPONSIBLE FOR DATA OVERAGES.

To Configure Data Usage:

1. Select the Applications tab and the Data Usage section, and enter the data usage fields, such as monthly limit (in GB or MB) and the day of the month that starts the cellular billing cycle.

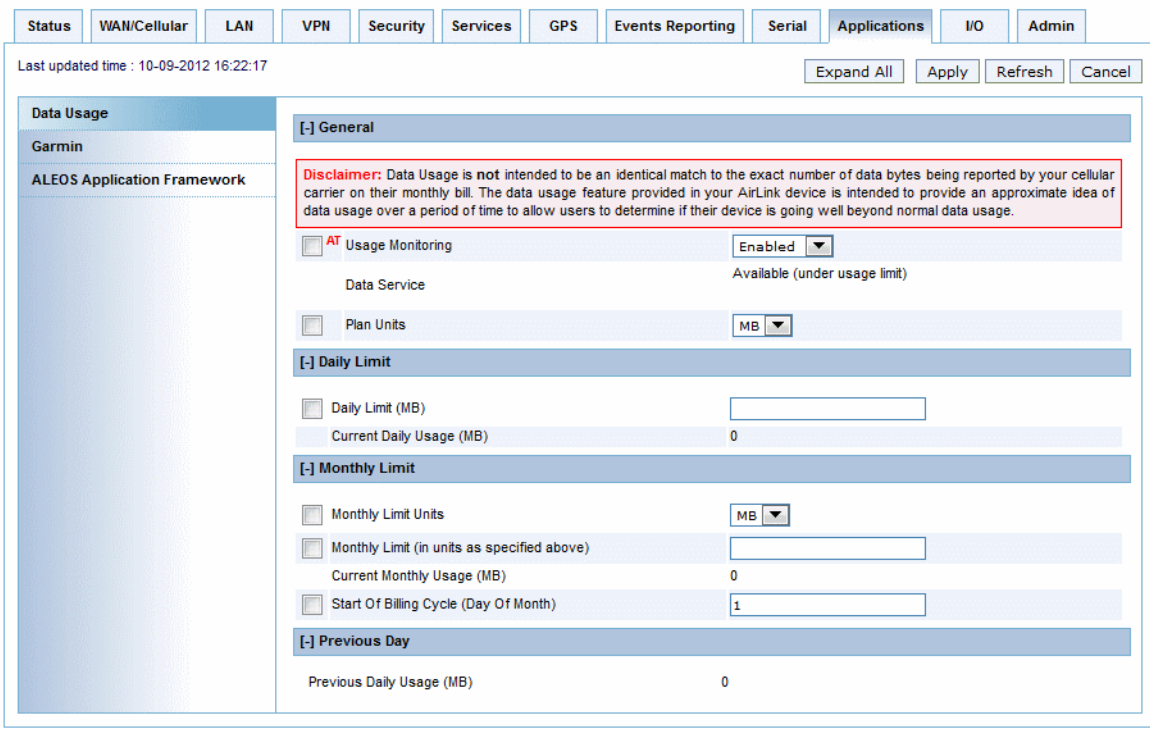


Figure 12-1: ACEmanager: Applications: Data Usage

Field	Description
General	
Usage Monitoring	Use this field to enable or disable data usage monitoring. Options are: • Disable (Default) • Enable
Data Service	If Data Service is on, “Available” appears on the user interface. If data usage exceeds the configured data limit, “Not Available” appears on the screen.
Plan Units	Select the units used for your data plan. The options are: • MB—Megabytes (Default) • KB—Kilobytes

Field	Description
Daily Limit	
Daily Limit (MB)	This is the user-specified daily data usage (in MBs) limit (24 hour limit). You can specify data usage limits on a daily or monthly basis. A limit is essentially a threshold that can trigger the software to take a user-specified action if the usage goes above the threshold. *Note: The Daily Limit value MUST be expressed as an integer (i.e., a whole number) and NOT as a fraction (e.g., "3.5").* **Caution:** *Data usage limits are approximate and based on reporting conditions in ALEOS. Data usage may run over the amount set in this field before ALEOS takes the specified action.* **Tip:** *ALEOS reads the data usage every 3 to 5 minutes. If you are using an application that requires high data usage, you can set an alert to warn you when data usage reaches a safe limit that takes into account the amount of data expected over the 3 to 5 minutes between data usage readings. For information on how to set an alert, see* *Events Reporting Configuration on page 207.*
Current Daily Usage (MB)	Displays the current daily data usage (in MBs). For example, if the daily limit is 60, the current daily usage should not exceed 60. The usage limit is 90%. You cannot access the cellular world if you exceed the limit. You can, however, Telnet, OTA, etc.
Monthly Limit	
Monthly Limit Units	Select an MB (default) or GB unit for monthly data usage.
Monthly Limit	This is the user-specified monthly data usage limit. Data usage accumulates on a monthly basis and on the date you specified (the "rolling month"). Data usage will accumulate during the month until the end of the next billing period at which point the data usage totals will be reset. *Note: The Monthly Limit value MUST be expressed as an integer (i.e., a whole number) and NOT as a fraction (e.g., "3.5")* **Caution:** *Data usage limits are approximate and based on reporting conditions in ALEOS. Data usage may run over the amount set in this field before ALEOS takes the specified action.*
Current Monthly Usage (MB)	Displays the current monthly data usage
Start of Billing Cycle (Day of Month)	Enter the desired start of the billing cycle. For example, 3 (Day 3 of every month)

Field	Description
Previous Day	
Previous Daily Usage (MB)	Shows the data usage for the previous day (in MB)

2. Select the Events Reporting tab and configure a data usage threshold. The threshold is specified as a percentage value of the monthly or daily limit. For example, if you have specified 5 GB as the monthly limit, and the threshold is set at 80%, then the threshold is reached when 4 GB of data usage is reached.

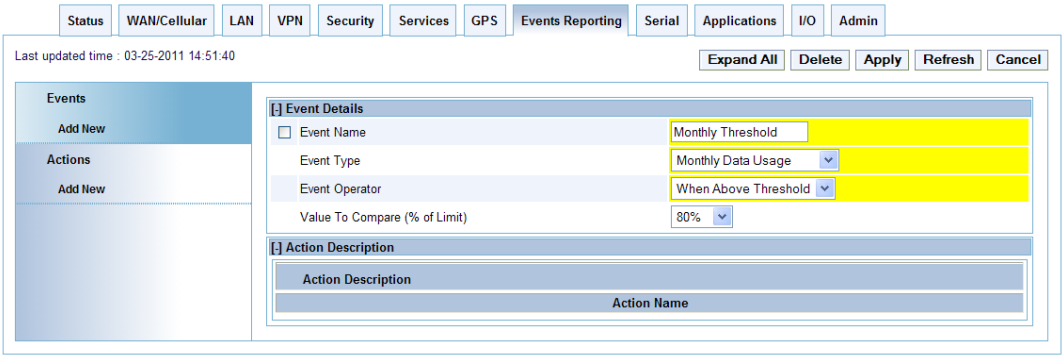


Figure 12-2: ACEmanager: Events Reporting > Events

3. Select the Actions group under Events Reporting tab, and specify an action to be performed when the Event is triggered.

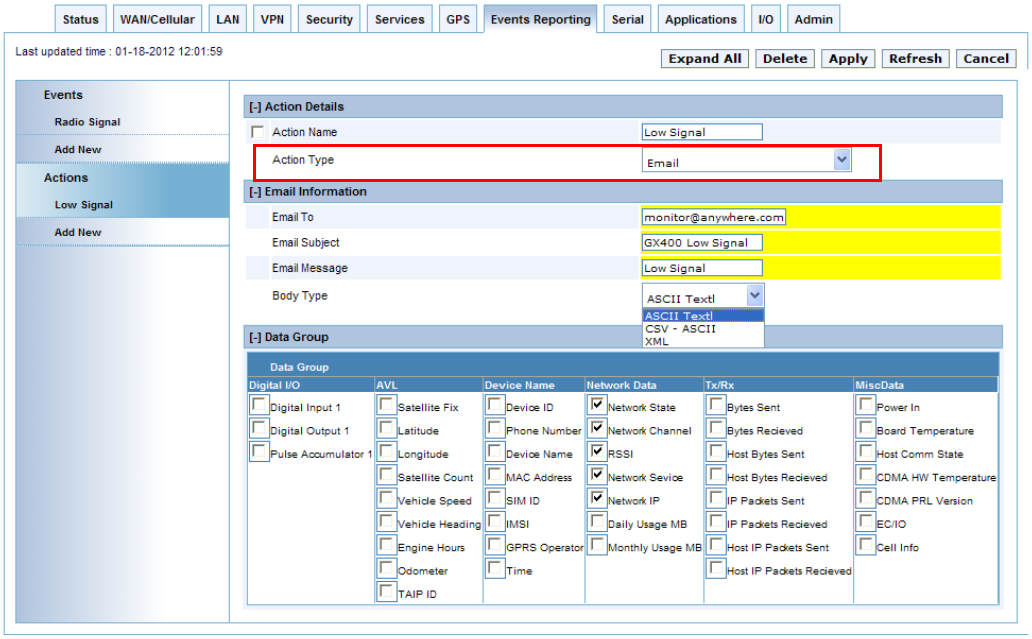


Figure 12-3: ACEmanager: Events Reporting > Actions

4. Select the Events group page again to associate the Data Usage Action with the Data Usage Event.

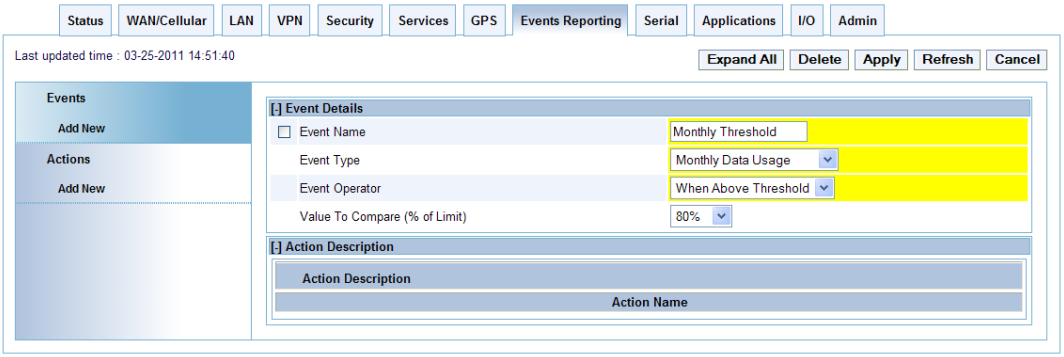


Figure 12-4: ACEmanager: Events Reporting > Events

Note: Daily and monthly limits will reset at the end of the billing cycle.

Once the data plan limit is reached, you may want to turn off cellular communication with any user devices connected to the host port until the next billing cycle starts.

To configure the device to turn off services, another event and action must be configured.

If you decide to disable the events and actions associated with the Data Usage feature, then the Data Usage Events must be deleted.

To turn off services on the data plan when the limit is reached:

1. Configure an event and an action. The event (shown below) is triggered when 100% of the monthly plan limit is reached.

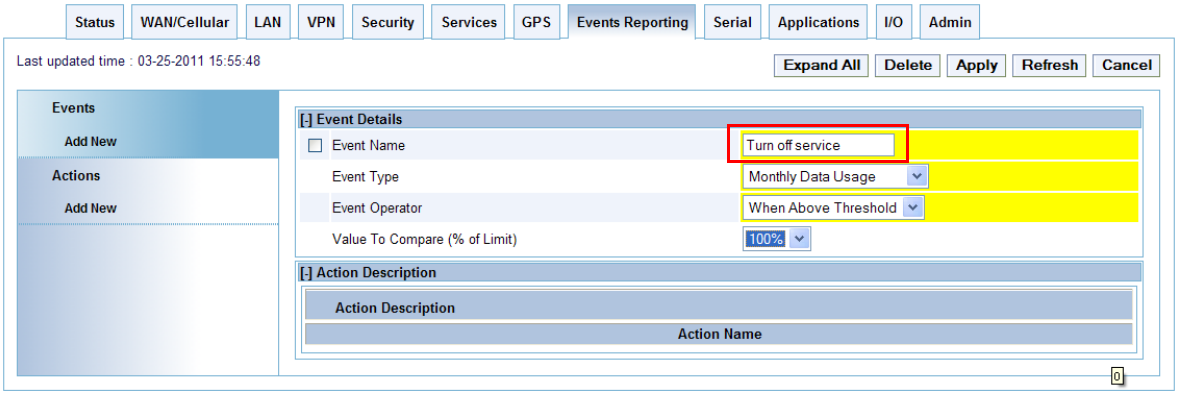


Figure 12-5: ACEmanager: Events Reporting > Events >Turn off Service

2. Create an action to turn off the services. When triggered, this action will prevent cellular communication to any user device connected to a host port.

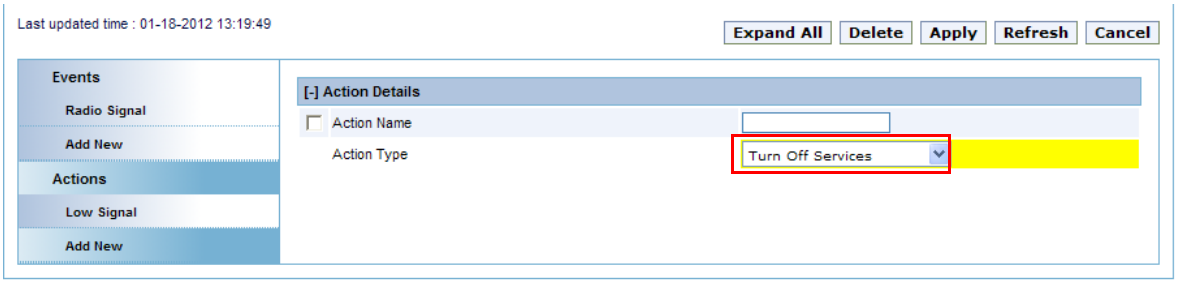


Figure 12-6: ACEmanager: Events Reporting > Actions > Add New

Garmin

Garmin provides navigation devices for versatile fleet monitoring solutions. AirLink devices provide Internet access to Garmin devices and a mechanism to enable via cellular. ALEOS also monitors links to the Garmin device and communication between the Garmin device and the server.

To configure Garmin in ACEmanager:

1. Under the Applications > Garmin tab, set the Garmin Device Attached feature to Enabled.

Figure 12-7: ACEmanager: Applications > Garmin

2. Set the Host Mode to TCP. Under the Serial > Port Configuration tab, set the Startup Mode Default parameter to TCP.

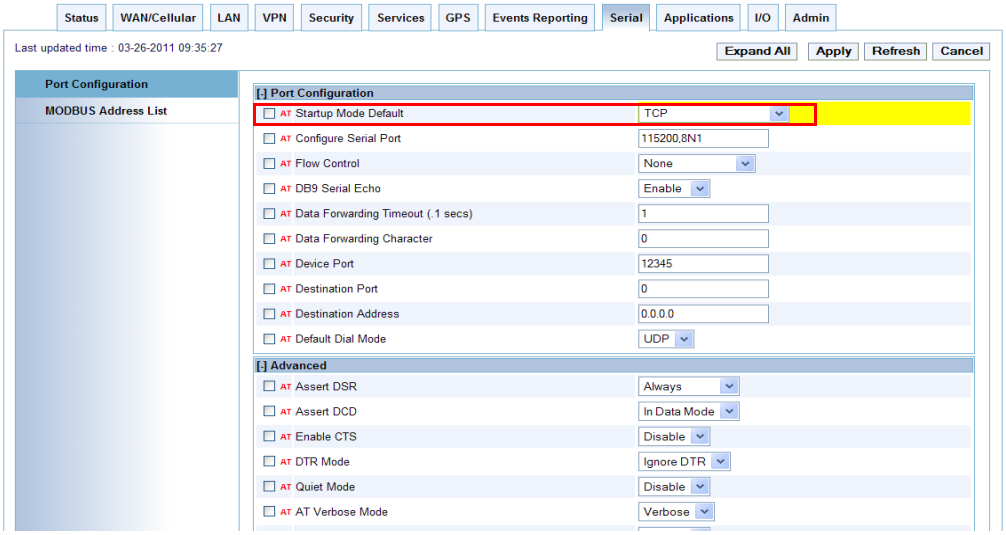


Figure 12-8: ACEmanager: Serial > Port Configuration

3. Set the Server Address and Port for TCP. Under the Serial > Port Configuration tab, set the Destination Port and the Destination Address to the port and address of the AVL server that the TCP application will be communicating with.

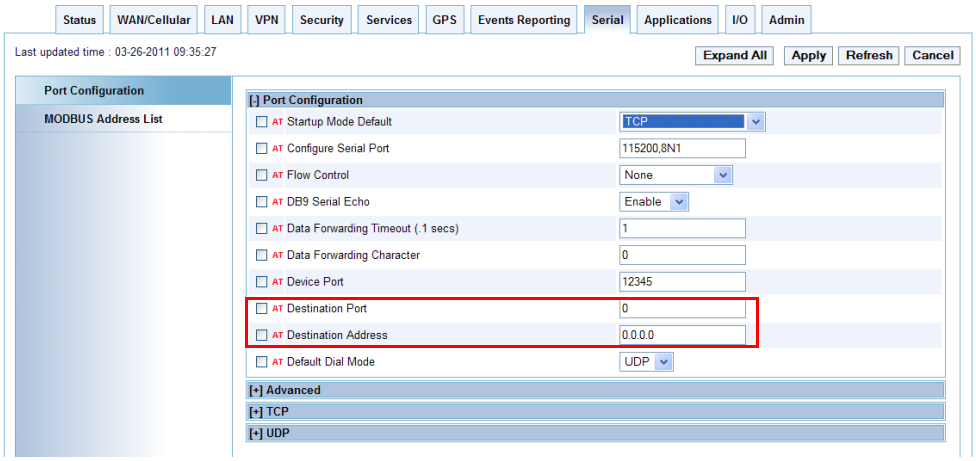


Figure 12-9: ACEmanager: Serial > Port Configuration

4. Configure the serial port. To communicate with Garmin:
   - Input **9600, 8N1** in Configure Serial Port
   - Select **None** in Flow Control
   - Select **Ignore DTR** in DTR Mode.

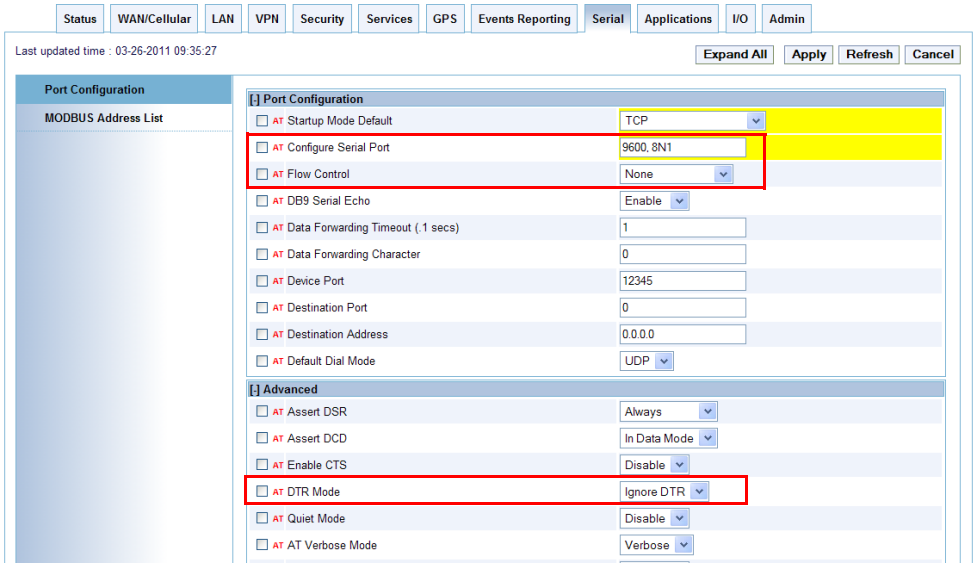


Figure 12-10: ACEmanager: Serial > Port Configuration parameters

5. Check the Garmin's communications status under the Status > Applications tab. Garmin data service states are:
   - Not Enabled — Not acknowledged by the AVL server

- Enabled — Acknowledged by the AVL server.

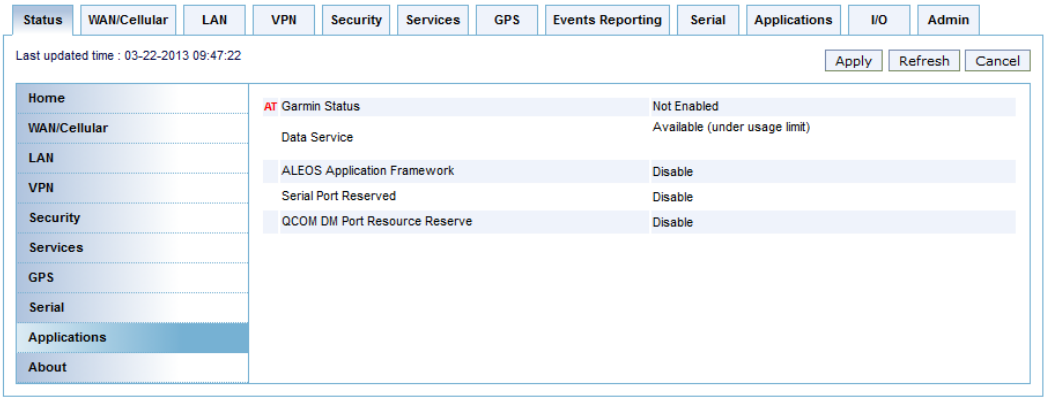


Figure 12-11: ACEmanager: Status > Applications > Garmin Status

6. Reboot the AirLink device to apply the changes. The “Garmin Status” now appears:
   - Enabled — Acknowledged by the AVL server.

*Note: The Garmin Status field appears **only** if the Garmin application is Connected.*

ALEOS Application Framework

ALEOS Application Framework (ALEOS AF) allows you to develop your own applications to run inside an AirLink device and leverage the AirVantage M2M Cloud Platform (www.sierrawireless.com/AirVantage) or a customer-developed server platform. Embedded and server application developers can start using ALEOS AF by accessing the Sierra Wireless Developer Zone (http://developer.sierrawireless.com/ALEOS_AF).

You may want to reserve the serial port for an ALEOS AF application. To do so, select Enable in Applications > ALEOS Application Framework > Serial Port Reserved.

It is not necessary to reserve the serial port before activating ALEOS AF.

Reserving the serial port is mandatory only if the ALEOS AF application will be using the serial port.

Note: When you reserve the serial port for ALEOS AF, it cannot be used for any other serial-related ALEOS features.

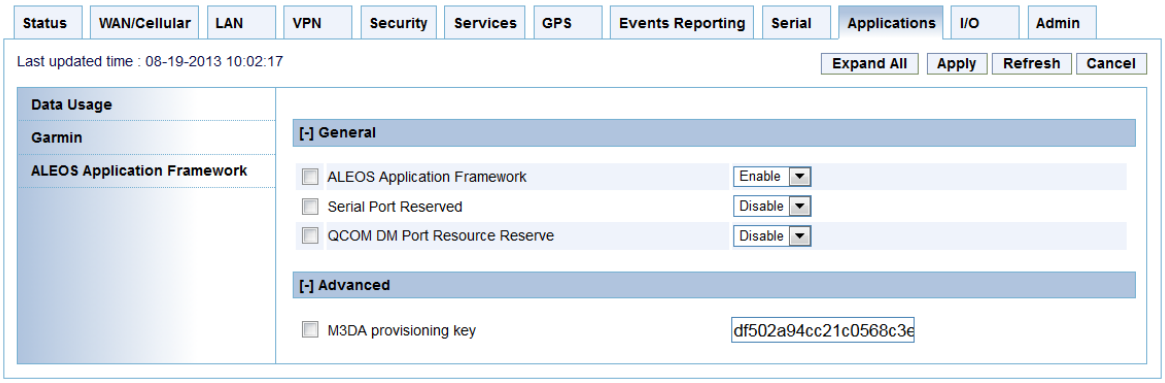


Figure 12-12: ACEmanager: Applications > ALEOS Application Framework

Field	Description
General	
ALEOS Application Framework	Enable or disable (default) the ALEOS Application Framework (ALEOS AF). If enabled, ALEOS AF starts at boot time. When the Reset to Factory default button on the Admin > Advanced page is pressed, ALEOS AF is disabled.
Serial Port Reserved	Select Enable to reserve the serial port for ALEOS AF. When this field is set to Enable, the serial port cannot be used for any other serial-related ALEOS features. The options are: • Disable (default) • Enable
QCOM DM Port Resource Reserve	Reserves the QCOM DM port for ALEOS AF applications. Options are: Enable (Reserve access for ALEOS AF) or Disable (Reserve access for ALEOS). Default: Disable
Advanced	
M3DA provisioning key	AAF now includes the M3DA provisioning key field. This field only appears if ALEOS AF is enabled. M3DA is the communication protocol used by AAF to send/receive data from AVMS. The M3DA provisioning key field contains the current M3DA provisioning key. Upon modification the M3DA keys are re-generated.

13: I/O Configuration

13

The I/O tab in ACEmanager is applicable across all Sierra Wireless AirLink devices that feature I/O ports.

You can use the input/outputs on AirLink devices to generate reports based on a threshold being crossed, a switch being open or closed, or the number of times a switch has changed its state.

Use the Events Reporting screen to configure reports. (See Events Reporting Configuration on page 207.) Use the I/O screen to view the current state of the analog and digital inputs, to turn the relays on and off, and to configure the units you want used in the reports based on analog inputs.

Analog inputs

Analog inputs monitor a voltage range in small increments. This allows you to monitor equipment that reports status as an analog voltage. Examples include:

- Power supply voltage
- Temperature, weight, volume, flow represented as voltage
- An incremental gauge with a voltage output
- Vehicle battery voltage

Using Event Reporting, you can create event thresholds, which when crossed (either higher or lower) generate a report to a defined external system. See Events Reporting Configuration on page 207.

The raw data for the changes being monitored is in volts, but you can use the I/O Configuration screen in ACEmanager to convert voltage to the desired units of measurement.

Digital inputs

Digital inputs monitor contact closures on a switch. This allows you to monitor changes such as:

- When a door or latch is open or closed
- When a container is full or empty
- When a switch or valve is open or closed
- The level of fuel in a vehicle (connected to an on/off sensor)
- When the trunk of a vehicle is opened or closed

You can use Events Reporting to generate reports and actions based on the digital input values.

Volts	Interpreted as
-0.5 – 1.2	Digital 0
2.2 – 30	Digital 1

Relay outputs

You can use relay outputs to trigger an intermediary switch and change the state of equipment.

AirLink GX Series device

The AirLink GX Series device without the I/O X-Card installed:

- Has one digital input or one relay output (configurable)
- Does not support analog input

The AirLink GX Series device with the I/O X-Card installed has:

- Five digital inputs or five relay outputs (configurable)
- Four analog inputs

Note: The fields for configuring the additional digital inputs/relay outputs are only available if you have an AirLink GX Series device with an I/O X-Card installed.

LS300

The LS300 has one pin that can be used as a digital input, relay output, or analog input.

More information

For more information on the basic features of the I/O settings for your AirLink device, refer to the applicable AirLink device user guide.

For more information on setting up reports, see Events Reporting Configuration on page 207.

Note: Changes to the relay outputs go into effect immediately. No reboot of the AirLink device is necessary. A reboot is required after configuring the transformed analog values. (See Transformed Analog on page 258.)

Current State

The Current State screen allows you to view the current values (as of the last refresh) of analog and digital inputs, pulse counts for digital inputs, and raw and transformed values for analog inputs. You can also use this screen to change the current values for Relay outputs. This change occurs immediately without a reboot.

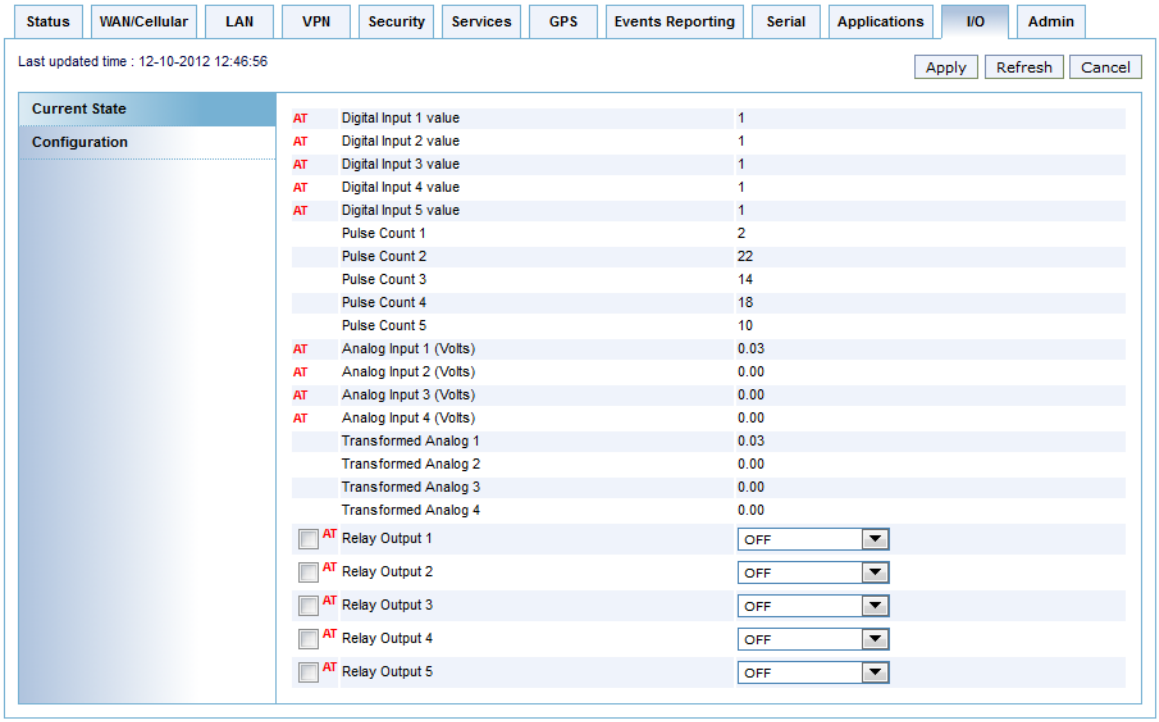


Figure 13-1: ACEmanager: I/0 > Current State (GX Series device with I/O X-Card)

Table 13-1: I/O: Current State

Command	Description
Digital Input # value	Query individual digital inputs. The digital inputs report either a 0 (open) or 1 (closed). • n= digital Input number *Note: Five digital inputs are available on an the AirLink GX Series device with an I/O X-Card. Otherwise, there is one digital input value.* You can also use an AT command to read these values. See *DIGITALIN[n]? on page 372.

Table 13-1: I/O: Current State

Command	Description
Pulse Count #	The pulse count increments when the input value changes from high to low. *Note: Five pulse counts are available on an AirLink GX Series device with an I/O X-Card. Otherwise, there is one pulse count.* *Note: To reset the pulse count to zero, reset the device to the factory defaults.*
Analog Input # (Volts)	Shows the current state of individual analog inputs The analog inputs report the voltage in volts. Range is 0–30 volts. You can also use an AT command to read these values. See *ANALOGIN[n]? on page 371.
Transformed Analog #	Shows the individual analog inputs in the units configured on the I/O Configuration screen
Relay Output #	Configure Relay Output signal. Options are: • OFF (default) The circuit is open. • Drive Action Low—equivalent to ON. The circuit is closed. *Note: Five relay outputs are available on an AirLink GX Series device with an I/O X-Card installed. Otherwise, there is one relay output.* *Note: If the same pin can be used for input or output, be aware that changing the output setting could change the input values. For pinout information for your AirLink device, refer to the applicable AirLink product user guide.* You can also use an AT command (see *RELAYOUT[#] on page 372), an SMS command (see [prefix]relay x y on page 378), or a RAP command (refer to the Remote Application Protocol User Guide) to configure this field.

Pulse Count

Pulse Count details:

- Pulses are counted on falling edge (high to low).
- Repeated pulses cannot be counted when the device is powered off, or being reset. However, a single change in state while the device is powered off or being reset is counted properly.
- To reset the pulse count to zero, reset the device to the factory defaults.

Configuration

This screen allows you to configure the initial relay settings and to transform units of measurement for the analog inputs from volts to a more appropriate unit, if applicable. Generated reports use the transformed value configured on this screen.

Refer to the user guide for your AirLink products for pinout information.

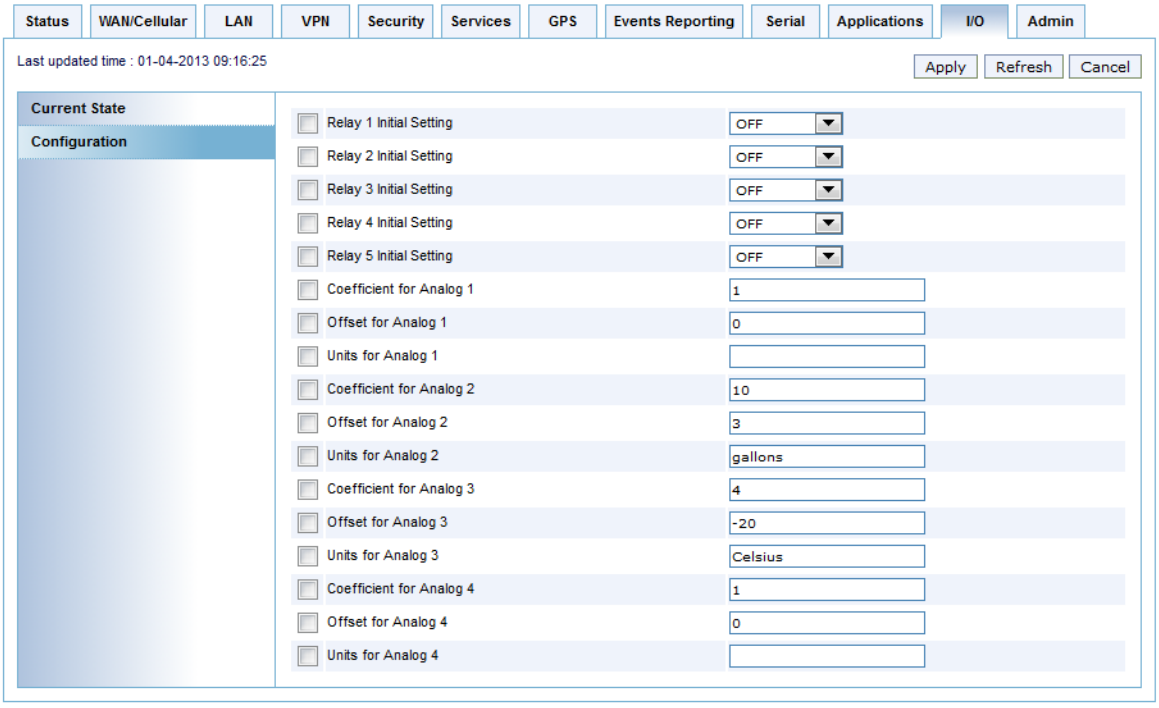


Figure 13-2: ACEmanager: I/O > Configuration

Field	Description
Relay # Initial Setting	The initial relay value when the AirLink device is powered on Options are: • ON • OFF (default) • Last Value (The value remains the same as it was before the AirLink device was powered down). When you change this field, the corresponding digital input value on this screen reflects the change after a screen refresh.
Coefficient for Analog #	This value may be found in the user guide for the equipment you want to monitor, or you can calculate it from information in the user guide. If this information is not available in the documentation that came with the equipment you want to monitor, contact the manufacturer. For an example of how to calculate the coefficient, see Transformed Analog on page 258.

Field	Description
Offset for Analog #	The offset (difference) between 0 volts and the equivalent value for the desired unit of measurement
Units for Analog #	The unit of measurement used in event reporting for the parameter being monitored by the analog input For example: degrees Celsius, degrees Fahrenheit, liters, mm, etc.

Transformed Analog

The raw analog data is displayed in volts. However, that is not always the most convenient unit of measurement to view the data. The I/O Configuration screen enables you to transform the voltage readings to a more convenient unit of measurement, for example degrees Celsius or Fahrenheit for temperature, liters for volume, etc.

Step 1—Coefficient and Offset

Before you configure ACEmanager, you need to locate or calculate the coefficient and the offset values.

Consult the user documentation for the equipment you want to monitor. It should provide you with the coefficient to convert volts to the appropriate unit of measurement and the offset value (the difference between the equivalent value for 0 volts and 0), or provide information on equivalent values for voltage readings from which you can calculate the coefficient and offset. (If this information is not available in the user documentation, contact the manufacturer.)

For example, if the equipment monitors temperature, and has a scale from 0 volts to 30 volts, the equipment specifications should provide information similar to the following:

0 V is equivalent to - 20°C

30 V is equivalent to 100°C

This is expressed algebraically as follows:

$$a \times 0V + b = -20C$$

$$a \times 30V + b = 100C$$

where:

a = coefficient

b = offset

For this example, you can calculate a as follows:

$$(a \times 30V + b) - (a \times 0V + b) = 100C - (-20)$$

$$a \times 30V = 120V$$

$$a = 4$$

To calculate b, substitute a into the first equation above:

$$4 \times 0V + b = -20$$

$$b = -20$$

Step 2—Configure ACEmanager

For each of the analog inputs you want to configure:

1. In ACEmanager, go to I/O > Configuration.
2. Enter the values for the coefficient and offset. (In this example, the coefficient is 4 and the offset is -20.)
3. Enter the desired unit of measurement. (In this example, the unit of measurement is C, for degrees Celsius).

ACEmanager shows the value of the transformed analog input as temperature in C.

Change Password

For system security reasons, changing the default password of the AirLink device is highly recommended.

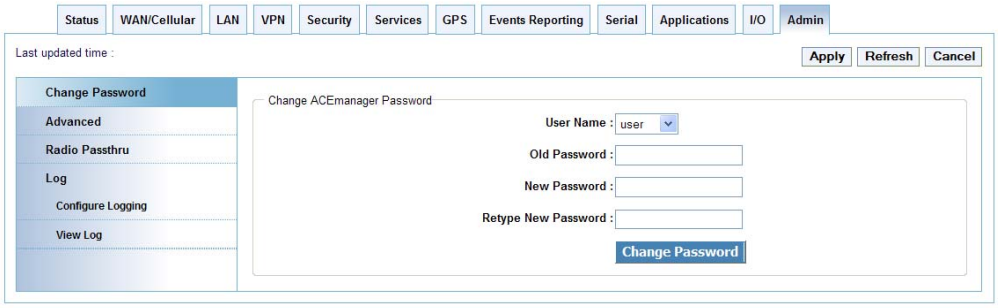


Figure 14-1: ACEmanager: Admin

To change the default password:

1. Select the User Name associated with the password you want to change: user, viewer, or sconsole.
2. Enter the old password.
3. Enter the new password twice.

   The password can be 4 to 32 characters long and can contain a mixture of letters, numbers, and/or special characters. The password is case sensitive.
4. Click Change Password.

You will be prompted to restart the AirLink Device. When the device has restarted, reconnect to ACEmanager and enter the new password.

Note: There are two user levels in the User Name drop-down menu. The 'user' has full administrator rights and can edit the configuration; the 'viewer' can only view the configuration and status of the device. Viewer can change the 'viewer' password. User can change both.

Advanced

Features which should be rarely changed and will affect the operation of the device are present on the Advanced screen.

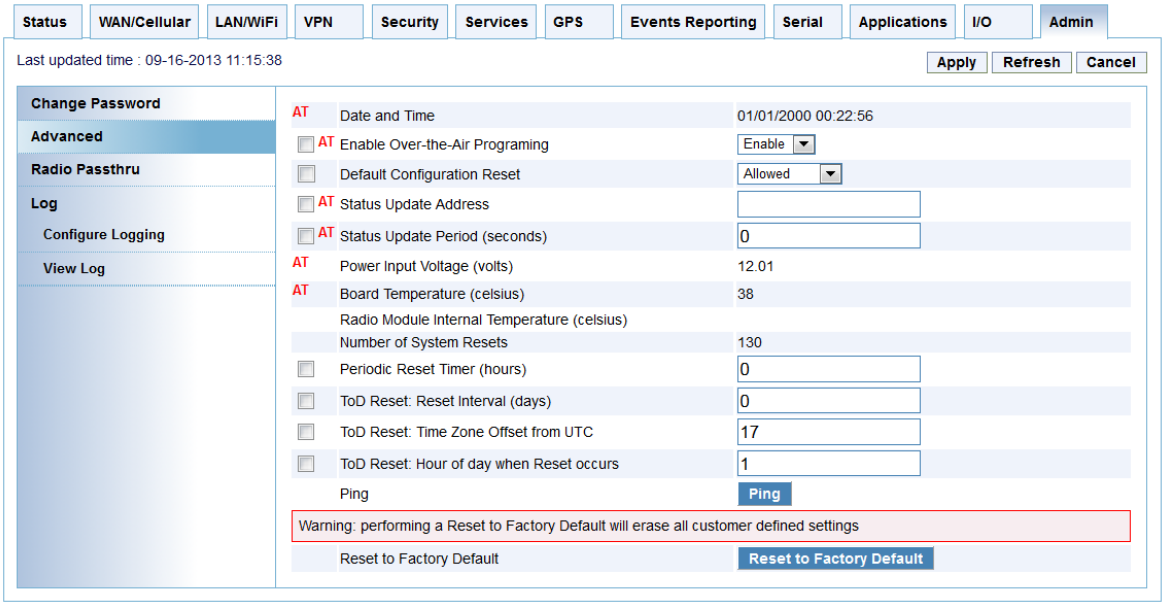
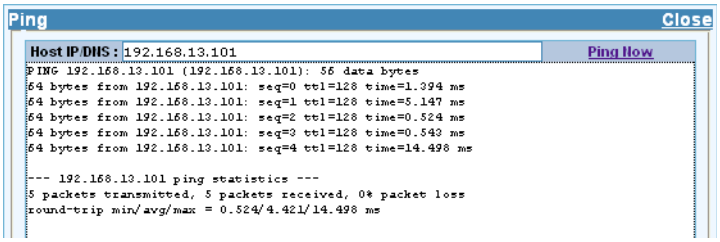


Figure 14-2: ACEmanager: Admin > Advanced

Field	Description
Date and Time	Queries the internal clock. The date and time are always specified in 24-hour notation (UTC). • mm/dd/yyyy= date in month/day/year notation • hh:mm:ss= time in 24-hour notation
Enable Over-the-Air Programming	Enables/disables over-the-air ALEOS software upgrading of the AirLink device. When Sierra Wireless releases a new version of ALEOS, you can upgrade your remote devices with Over-the-Air Programming (OPRG) enabled. • Enable (default) • Disable
Default Configuration Reset	Enables or disables the hardware reset button Sets the AirLink device to allow (or not allow) the hardware reset button to reset the device to the factory default settings. • Allowed—Pressing the hardware reset button for 10 seconds reboots the device and resets it to the factory defaults. • Not Allowed—Pressing the hardware reset button for 10 seconds reboots the device, but does **not** reset it to the factory defaults. *Note: Regardless of the setting selected in this field, you can still reset the device by clicking the "Reset to Factory Defaults" button in ACEmanager.*
Status Update Address	Enter the device Name/Port. Name is the domain name or IP address, and Port is the port of the device where the device status updates will be sent. This report can be sent to a LAN connected host (e.g., 192.168.13.100/1122) or a remote location (e.g., newb.eairlink.com/17000). The status parameters are sent in an XML format.

Field	Description
Status Update Period (seconds)	The time interval (in seconds) when a status update should be sent
Power Input Voltage (volts)	Displays the power input voltage in volts. If the input voltage ground is connected to the AirLink device case (without serial connection), this value reads .3 V (approx.) less; if ground is connected (with serial connection), the value reads .3 V (approx.) more.
Board Temperature (celsius)	Displays the board temperature in degrees (Celsius)
Radio Module Internal Temperature (celsius)	Displays the temperature of the internal radio module in degrees (Celsius).
Number of System Resets	Counter of the number of system resets over the life of the device or since the configuration was reset
Periodic Reset Timer (hours)	Resets the device after the specified number of hours. 0 = disabled
ToD Reset: Reset Interval in (days)	Number of days between resets 0 = Disabled Example: If this field is set to 3, the device resets every third day.
ToD Reset: Time Zone Offset from UTC	Time zone adjustment (Offset in easterly direction from UTC Time) Possible values are 0–23 Example: Pacific Standard Time would be 17
ToD Reset: Hour of day when Reset occurs	The local hour of the day when the reset occurs Possible values are 0–23 Example: 4 is 4:00 am
Ping	Use this button to confirm that a connected device is responding. **1.** Click Ping. **2.** In the pop-up window, enter the device IP address or DNS name and click Ping Now. 
Reset to Factory Default	Erases all customer-defined settings and resets all settings (passwords, LAN and WAN configuration, security settings, ALEOS Applications Framework, etc.) to the original factory settings. ALEOS AF is also reset to disabled.

Radio Passthru

Radio Passthru allows a direct connection, using USB, to the internal radio. Normal cellular radio operation is suspended while Radio Passthru is enabled.

Radio Passthru is generally used only in certain troubleshooting scenarios.

The hardware bypass will remain in effect until the ALEOS software resets either via ACEmanager command or the hardware Reset button.

Note: Because Radio Passthru is not USB/net or USB/serial, a different set of drivers are required to connect to the radio installed inside an AirLink device. Additionally, while it is possible to send AT commands to the radio using a terminal connection, there are software applications designed to communicate with the radio directly. If you need to use Radio Passthru, contact your Sierra Wireless AirLink representative to obtain the needed drivers and/or software application.

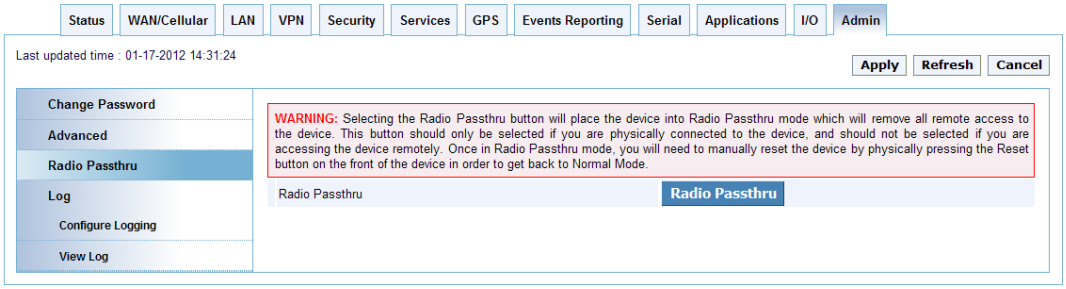

Status
WAN/Cellular
LAN
VPN
Security
Services
GPS
Events Reporting
Serial
Applications
I/O
Admin
Last updated time : 01-17-2012 14:31:24
Apply
Refresh
Cancel
Change Password
Advanced
Radio Passthru
Log
Configure Logging
View Log
WARNING: Selecting the Radio Passthru button will place the device into Radio Passthru mode which will remove all remote access to the device. This button should only be selected if you are physically connected to the device, and should not be selected if you are accessing the device remotely. Once in Radio Passthru mode, you will need to manually reset the device by physically pressing the Reset button on the front of the device in order to get back to Normal Mode.
Radio Passthru
Radio Passthru

Figure 14-3: ACEmanager: Admin > Radio Passthru

Log

The Log file is a system log of the AirLink device.

The Logging configuration screen enables you to configure log verbosity and display filtering. The View Log screen enables you to view and save logs. The logs are in plain text.

To configure what you want to include in the logs:

1. In ACEmanager, go to Admin > Log.

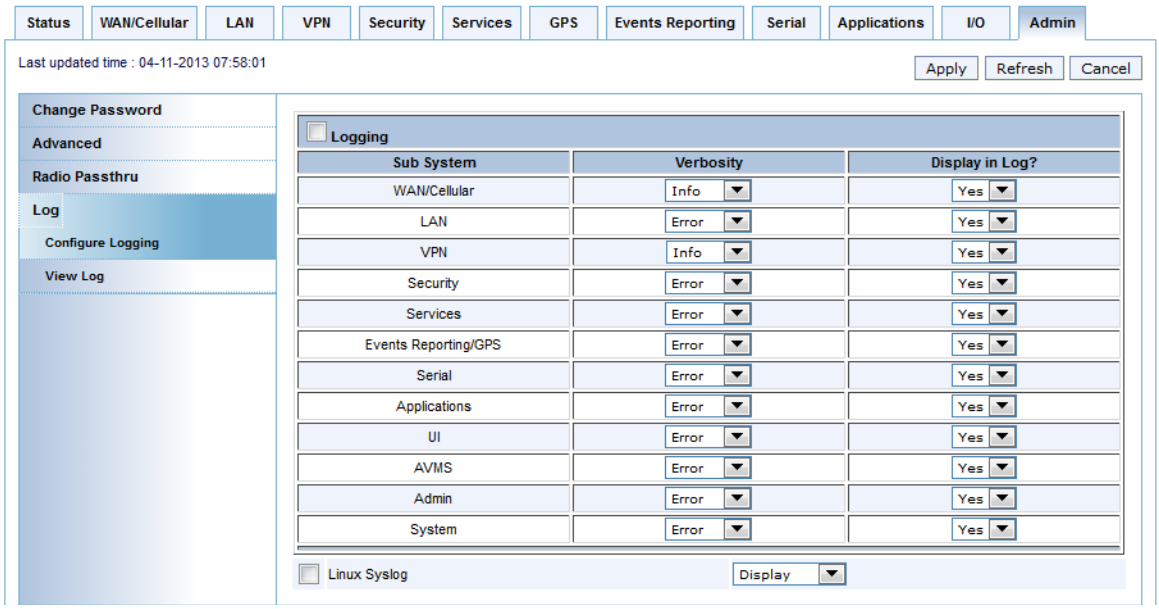


Figure 14-4: ACEmanager: Admin > Log, Configure Logging

2. For each subsystem listed:

   a. Select whether or not to display it in the log.

   Separate filters, based on subsystem and severity, are applied when the messages are generated and when the messages are displayed. Four severity levels are supported for filtering in the drop-down lists for verbosity:

   - Critical
   - Error
   - Info (information)
   - Debug

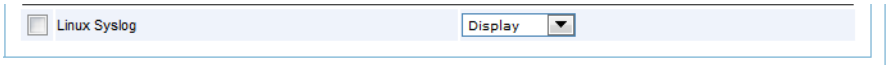
Note: The VPN Sub System only allows for Info and Debug. For maximum information, set the VPN verbosity to Debug.

   b. Select the verbosity level.

Note: Some log messages are only displayed if you display Linux Syslog. For example, If you are debugging a VPN or LAN setup, the relevant information is only displayed in the Linux Syslog.

3. Optional: To display Linux Syslog:

   a. Ensure that Display (default value) is selected the drop-down menu beside Linux Syslog.



4. Click Apply.
5. If you have changed any of the verbosity levels or the Linux syslog setting:

   a. Reboot the AirLink device.

b. Log into ACEmanager, go to Admin > Log.

6. Select View Logs from the menu on the left side of the window.

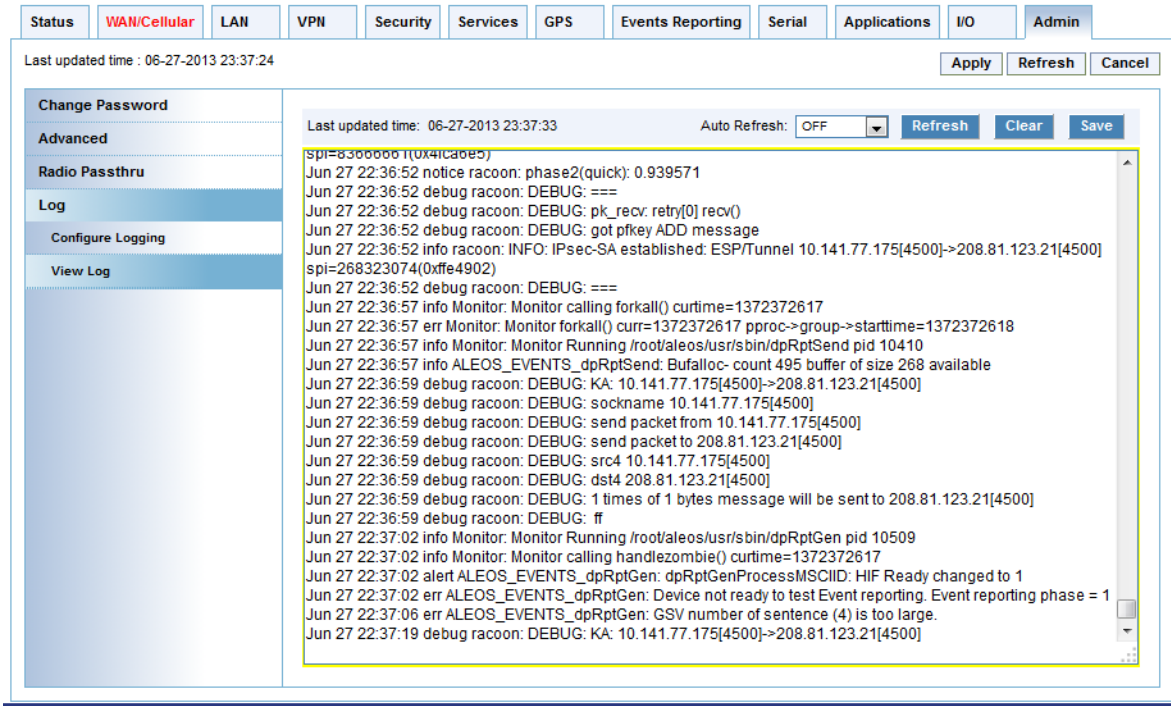

Status
WAN/Cellular
LAN
VPN
Security
Services
GPS
Events Reporting
Serial
Applications
I/O
Admin
Last updated time : 06-27-2013 23:37:24
Apply
Refresh
Cancel
Change Password
Advanced
Radio Passthru
Log
Configure Logging
View Log
Last updated time: 06-27-2013 23:37:33
Auto Refresh:
OFF
Refresh
Clear
Save
Jun 27 22:36:52 notice racoon: phase2(quick): 0.939571
Jun 27 22:36:52 debug racoon: DEBUG: ===
Jun 27 22:36:52 debug racoon: DEBUG: pk_recv: retry[0] recv()
Jun 27 22:36:52 debug racoon: DEBUG: got pfkey ADD message
Jun 27 22:36:52 info racoon: INFO: IPsec-SA established: ESP/Tunnel 10.141.77.175[4500]->208.81.123.21[4500]
spi=268323074(0xffe4902)
Jun 27 22:36:52 debug racoon: DEBUG: ===
Jun 27 22:36:57 info Monitor: Monitor calling forkall() curtime=1372372617
Jun 27 22:36:57 err Monitor: Monitor forkall() curr=1372372617 pproc->group->starttime=1372372618
Jun 27 22:36:57 info Monitor: Monitor Running /root/aleos/usr/sbin/dpRptSend pid 10410
Jun 27 22:36:57 info ALEOS_EVENTS_dpRptSend: Bufalloc- count 495 buffer of size 268 available
Jun 27 22:36:59 debug racoon: DEBUG: KA: 10.141.77.175[4500]->208.81.123.21[4500]
Jun 27 22:36:59 debug racoon: DEBUG: sockname 10.141.77.175[4500]
Jun 27 22:36:59 debug racoon: DEBUG: send packet from 10.141.77.175[4500]
Jun 27 22:36:59 debug racoon: DEBUG: send packet to 208.81.123.21[4500]
Jun 27 22:36:59 debug racoon: DEBUG: src4 10.141.77.175[4500]
Jun 27 22:36:59 debug racoon: DEBUG: dst4 208.81.123.21[4500]
Jun 27 22:36:59 debug racoon: DEBUG: 1 times of 1 bytes message will be sent to 208.81.123.21[4500]
Jun 27 22:36:59 debug racoon: DEBUG: ff
Jun 27 22:37:02 info Monitor: Monitor Running /root/aleos/usr/sbin/dpRptGen pid 10509
Jun 27 22:37:02 info Monitor: Monitor calling handlezombie() curtime=1372372617
Jun 27 22:37:02 alert ALEOS_EVENTS_dpRptGen: dpRptGenProcessMSCIID: HIF Ready changed to 1
Jun 27 22:37:02 err ALEOS_EVENTS_dpRptGen: Device not ready to test Event reporting. Event reporting phase = 1
Jun 27 22:37:06 err ALEOS_EVENTS_dpRptGen: GSV number of sentence (4) is too large.
Jun 27 22:37:19 debug racoon: DEBUG: KA: 10.141.77.175[4500]->208.81.123.21[4500]

Figure 14-5: ACEmanager: Admin > Log, View Log

Note: VPN info and debug information uses the term racoon (rather than VPN), as shown in Figure 14-5.

Note: If you toggle the "Display in Log?" field, clear and refresh the View Log page. (You do not need to reboot the device.)

Tip: *Use View Log for troubleshooting purposes (e.g., when setting up the IPsec configuration). The Log page allows you to establish the tunnel connection and monitor the results directly. To change the intervals at which the log is displayed, you can change the settings in Auto Refresh.*

Actions on the View Log screen include:

- Auto Refresh — The drop-down menu allows you to set up an automatic log page refresh, and the interval between refreshes: 30 secs, 1 minute, or 2 minutes.
- Refresh button — Initiates a manual page refresh
- Clear button — Clears out the tunnels
- Save button — Creates a text file of the log

A: Windows Dial-up Networking (DUN)

Dial-up Networking (DUN) allows a computer or other device to use the serial port on your AirLink device to connect to the Internet or private network using PPP just like an analog device using a standard phone line.

Note: Dial-up Networking is not available for the AirLink LS300.

Caution: *To install any driver on your computer, you may need to be logged in as Administrator or have Administrator privileges for your login.*

Microsoft Windows 7 is used in the examples below. The device driver installation and DUN setup and configuration is similar in other Microsoft Windows operating systems, including Windows XP and Windows CE.

Note: If your device is new, or has recently been reset to factory default settings, ensure that the device has been on air at least once before being used with a DUN connection.

Installing a Device Driver

Connect the AirLink device

1. Connect the device to the computer with a DB-9 cable from one RS-232 port to the other.
2. Log in to ACEmanager.
3. Go to Serial > Port Configuration.
4. Set the DB9 Serial Echo field to Disable.
5. Reboot.

Note: You need to set the DB9 Serial Echo field echo to Disable any time you want to set up a PPP connection.

Install the driver

1. Select Start > Control Panel > Phone and Modem Options.

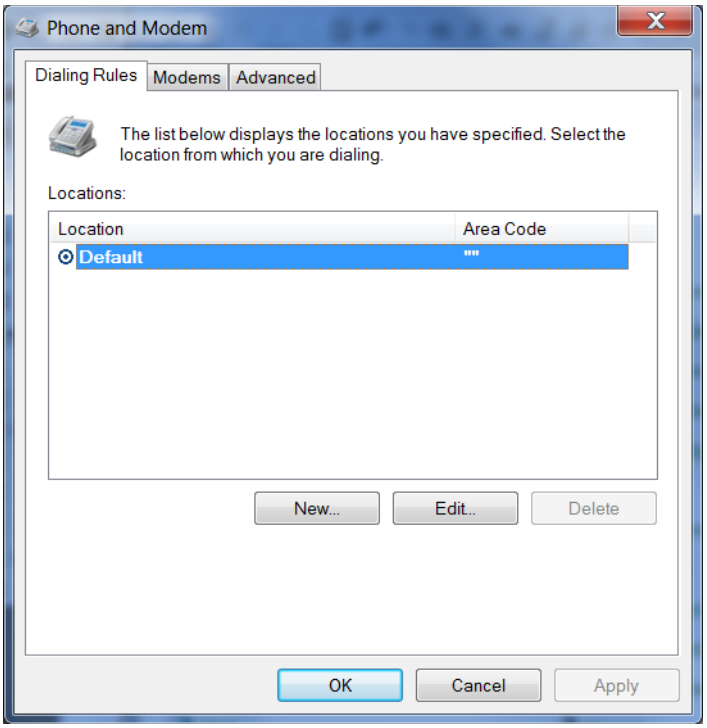


Figure A-1: Phone and Modem Options

2. Select the Modems tab.

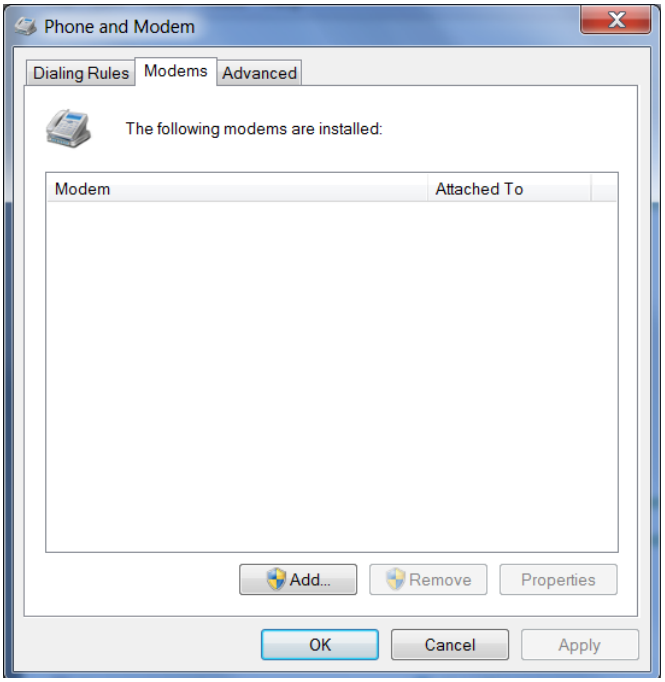


Figure A-2: Phone and Modem Options: devices

3. Click Add.

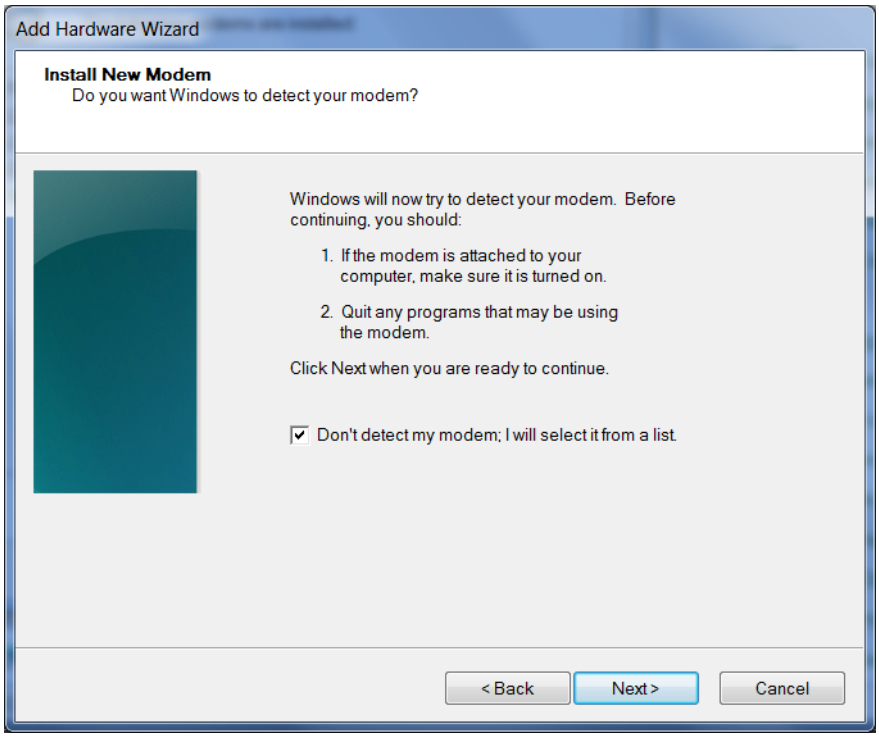

Add Hardware Wizard
Install New Modem
Do you want Windows to detect your modem?
Windows will now try to detect your modem. Before continuing, you should:
1. If the modem is attached to your computer, make sure it is turned on.
2. Quit any programs that may be using the modem.
Click Next when you are ready to continue.
Don't detect my modem; I will select it from a list.
< Back
Next >
Cancel

Figure A-3: Add Hardware Wizard

4. Select Don't detect my modem; I will select it from a list.
5. Click Next.

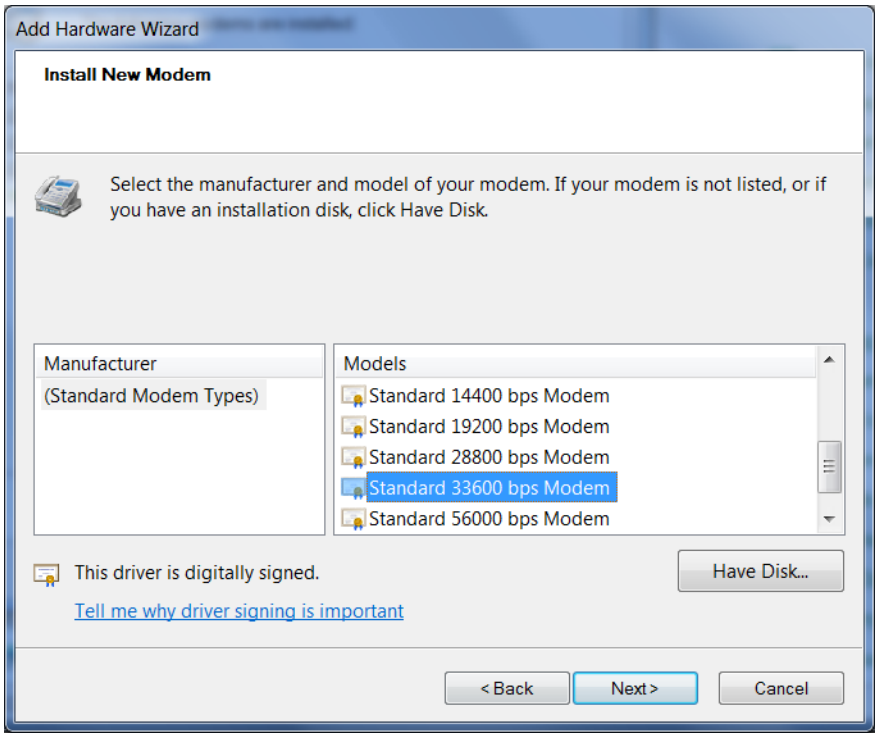

Add Hardware Wizard
Install New Modem
Select the manufacturer and model of your modem. If your modem is not listed, or if you have an installation disk, click Have Disk.
Manufacturer
(Standard Modem Types)
Models
Standard 14400 bps Modem
Standard 19200 bps Modem
Standard 28800 bps Modem
Standard 33600 bps Modem
Standard 56000 bps Modem
This driver is digitally signed.
Have Disk...
Tell me why driver signing is important
< Back
Next >
Cancel

Figure A-4: Add Hardware Wizard: Install New Modem

6. Under Manufacturer, select (Standard Modem Types).
7. Under Models, select Standard 33600 bps Modem.

Tip: *If you have the speed for your device configured as something other than the default, use the Standard device that matches the speed you configured.*

8. Click Next.

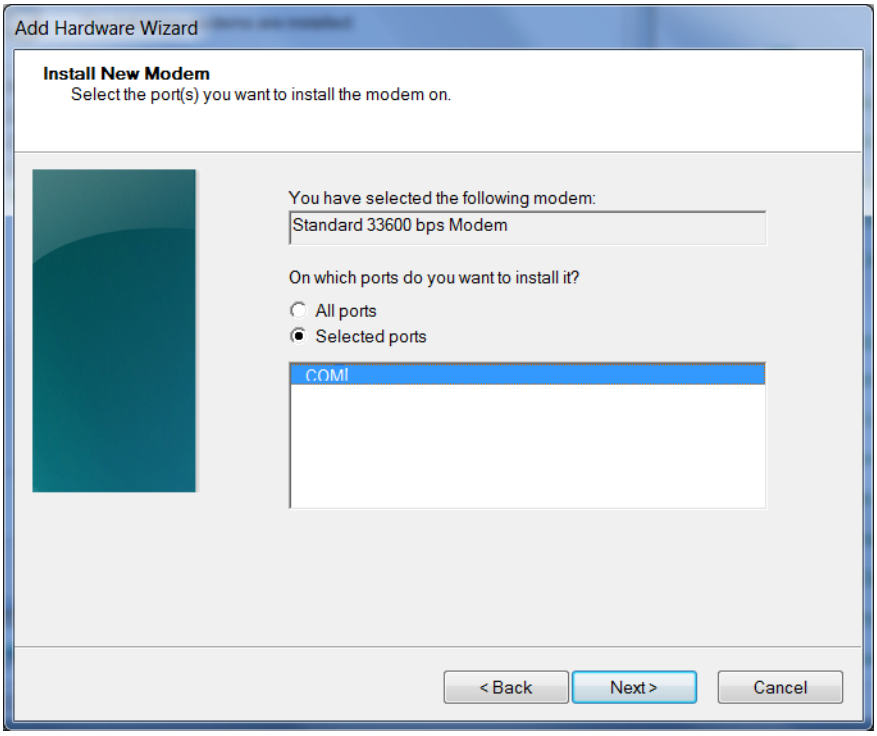

Add Hardware Wizard
Install New Modem
Select the port(s) you want to install the modem on.
You have selected the following modem:
Standard 33600 bps Modem
On which ports do you want to install it?
All ports
Selected ports
COM1
< Back
Next >
Cancel

Figure A-5: Add Hardware Wizard: Select Ports

9. Select Selected Ports.
10. Select the COM port the device is connected to (commonly COM1).
11. Click Next.

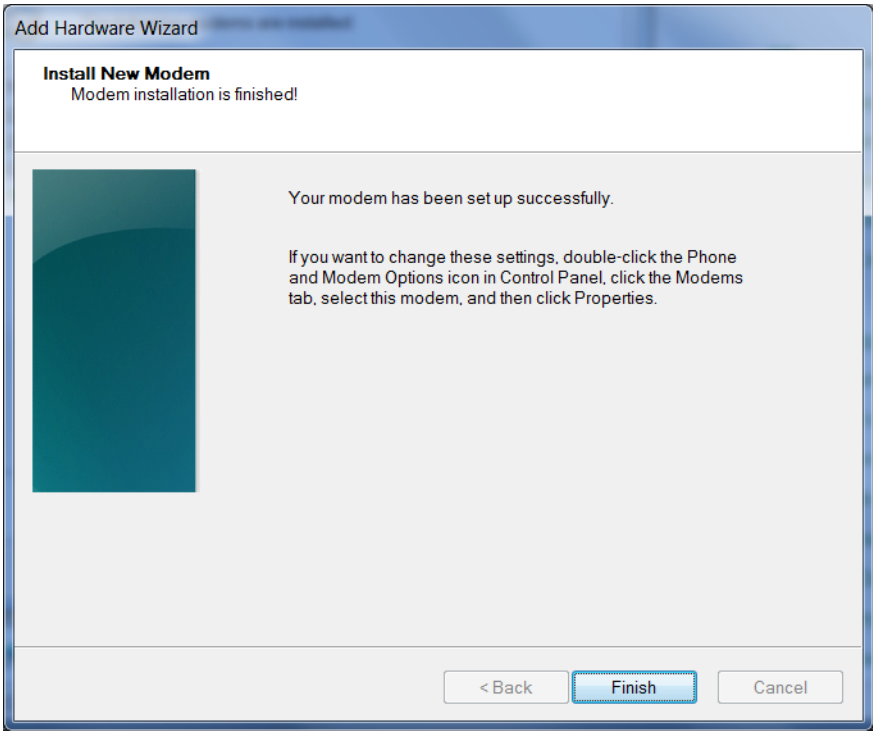

Add Hardware Wizard
Install New Modem
Modem installation is finished!
Your modem has been set up successfully.
If you want to change these settings, double-click the Phone and Modem Options icon in Control Panel, click the Modems tab, select this modem, and then click Properties.
< Back
Finish
Cancel

Figure A-6: Add Hardware Wizard: Finish

12. Once the device driver is installed, click Finish.

When you return to the Phone and Modem Options window, you should see the newly installed device “attached to” the correct COM port.

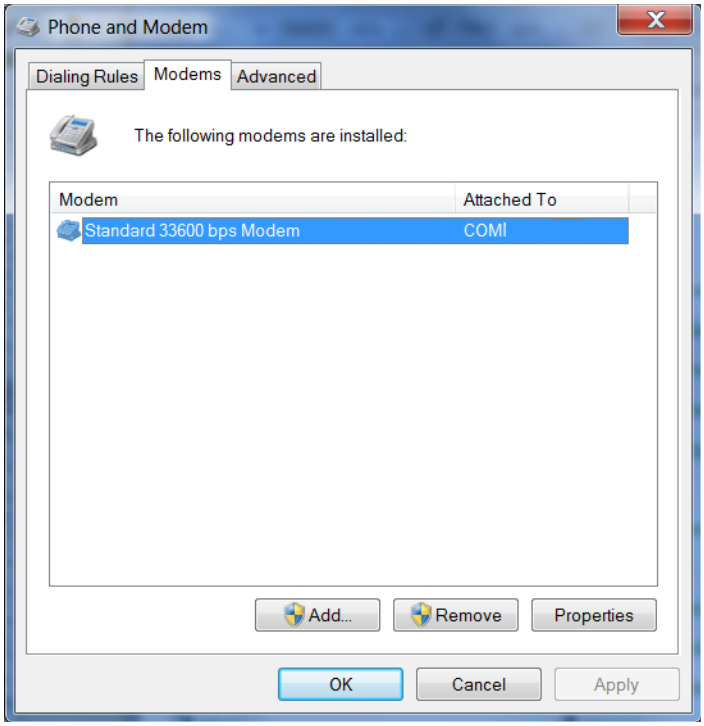


Figure A-7: Phone and Modem Options > Modems

13. Highlight the modem, and click Properties. The following window appears:

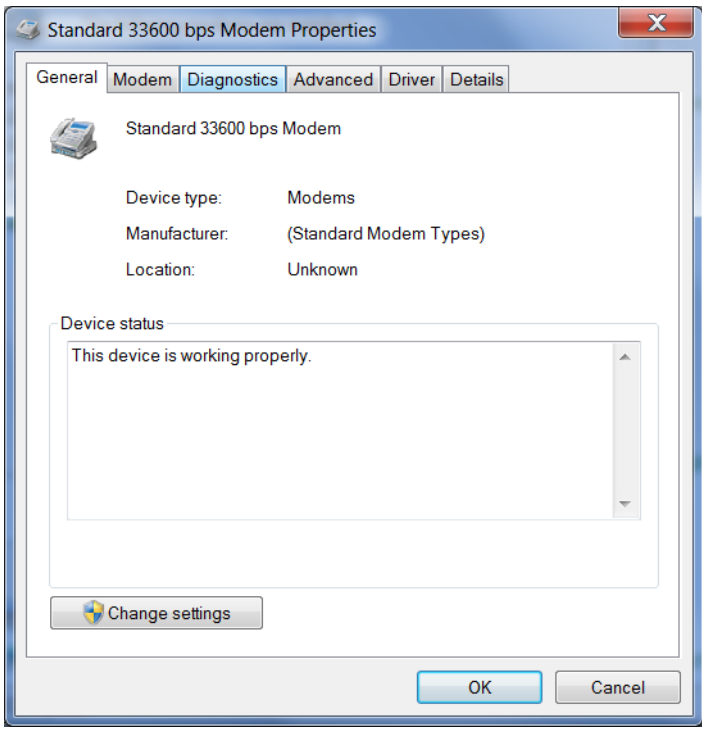


Figure A-8: Modem Properties

14. Select the Modem tab.

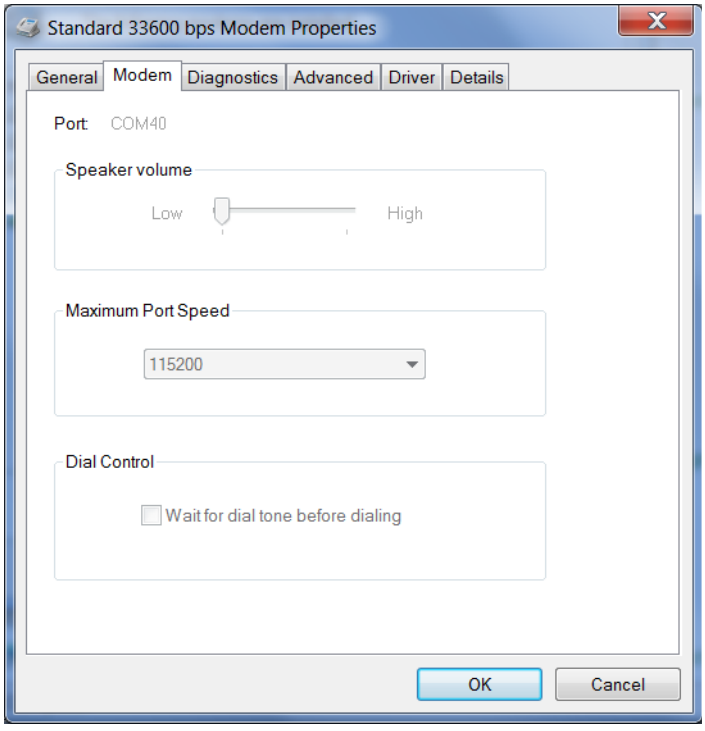


Figure A-9: Modem Properties > Modem

15. Confirm that the Maximum Port Speed is set to 115200 (default).

16. Click OK to exit.
17. Click OK again to exit out of the Phone and Modem Options.
18. Go to Start > Control Panel > Device Manager.

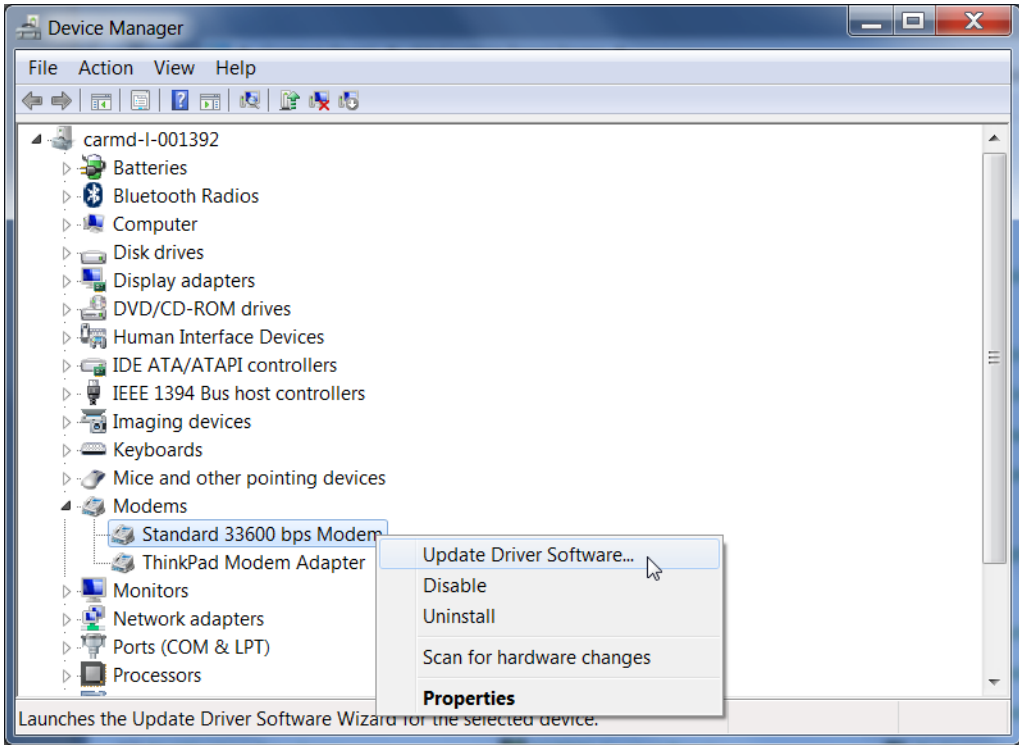


Figure A-10: Device Manager

19. Under Modems, highlight Standard 33600 bps Modem. Right-click and select Update Driver Software....

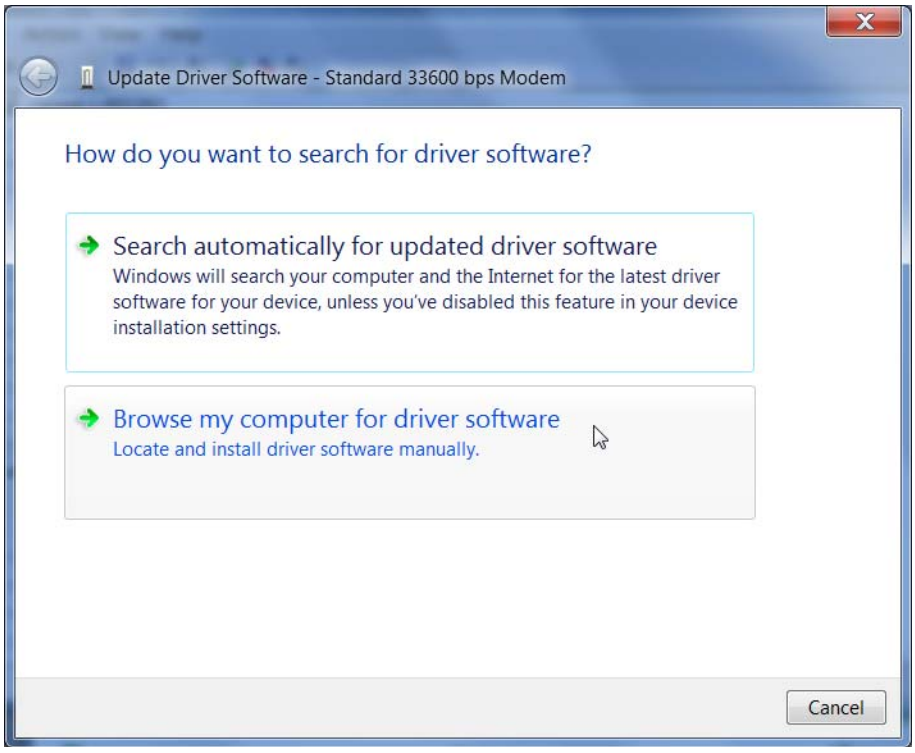

Update Driver Software - Standard 33600 bps Modem
How do you want to search for driver software?
Search automatically for updated driver software
Windows will search your computer and the Internet for the latest driver software for your device, unless you've disabled this feature in your device installation settings.
Browse my computer for driver software
Locate and install driver software manually.
Cancel

Figure A-11: Update Driver Software—Browse

20. Select Browse my computer for driver software.

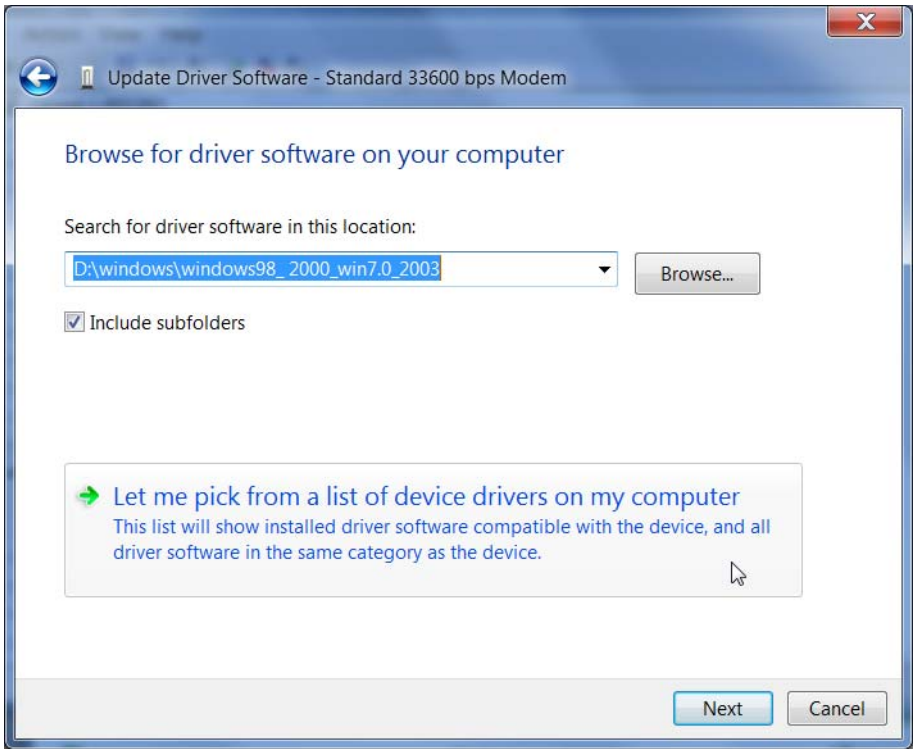

Update Driver Software - Standard 33600 bps Modem
Browse for driver software on your computer
Search for driver software in this location:
D:\windows\windows98_2000_win7.0_2003
Browse...
Include subfolders
Let me pick from a list of device drivers on my computer
This list will show installed driver software compatible with the device, and all driver software in the same category as the device.
Next
Cancel

Figure A-12: Update Driver Software—Let me pick...

21. Select Let me pick from a list of device drivers on my computer.

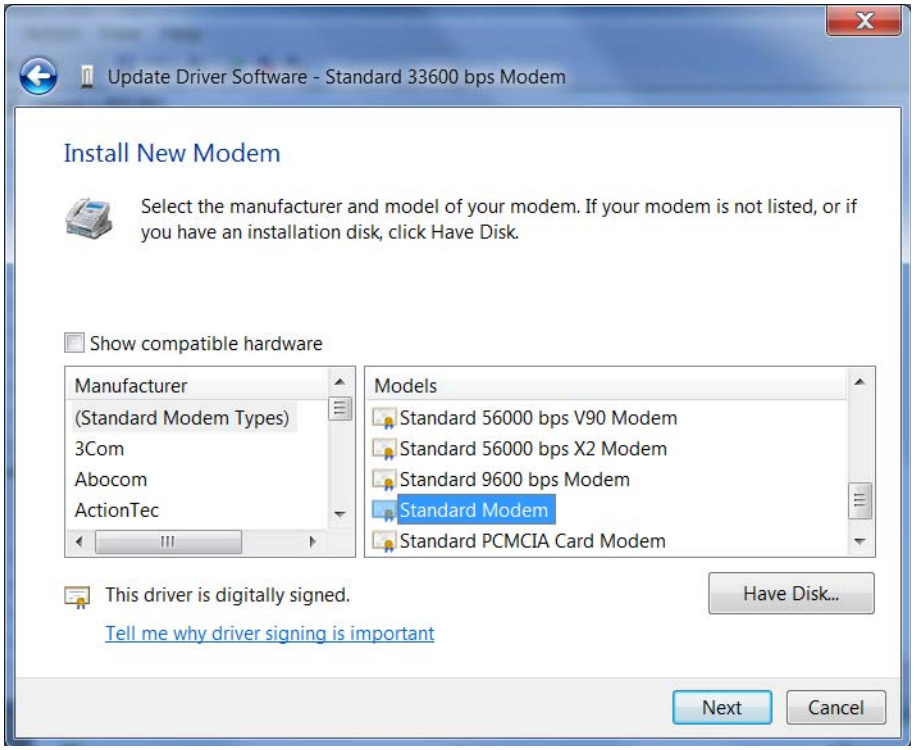

Update Driver Software - Standard 33600 bps Modem
Install New Modem
Select the manufacturer and model of your modem. If your modem is not listed, or if you have an installation disk, click Have Disk.
Show compatible hardware
Manufacturer
(Standard Modem Types)
3Com
Abocom
ActionTec
Models
Standard 56000 bps V90 Modem
Standard 56000 bps X2 Modem
Standard 9600 bps Modem
Standard Modem
Standard PCMCIA Card Modem
This driver is digitally signed.
Have Disk...
Tell me why driver signing is important
Next
Cancel

Figure A-13: Update Driver Software—Select Standard Modem

22. Deselect Show compatible hardware.
23. Under Manufacturer, select (Standard Modem Types).
24. Under Models, select Standard Modem.
25. Click Next.

    If you see an Update Driver Warning, click Yes.

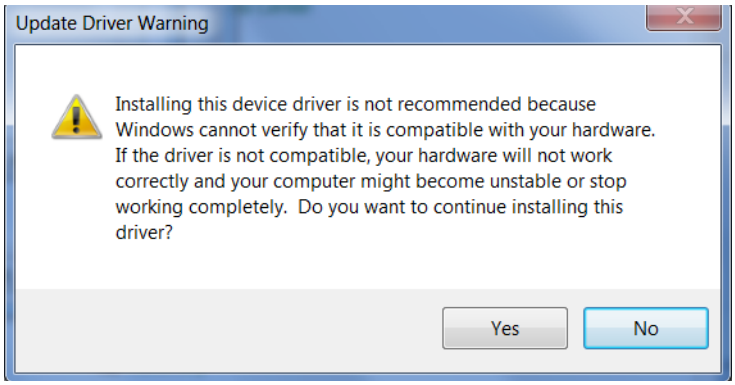

Update Driver Warning
Installing this device driver is not recommended because Windows cannot verify that it is compatible with your hardware. If the driver is not compatible, your hardware will not work correctly and your computer might become unstable or stop working completely. Do you want to continue installing this driver?
Yes
No

Figure A-14: Update Driver Software—Warning

The software driver updates and the following window appears:

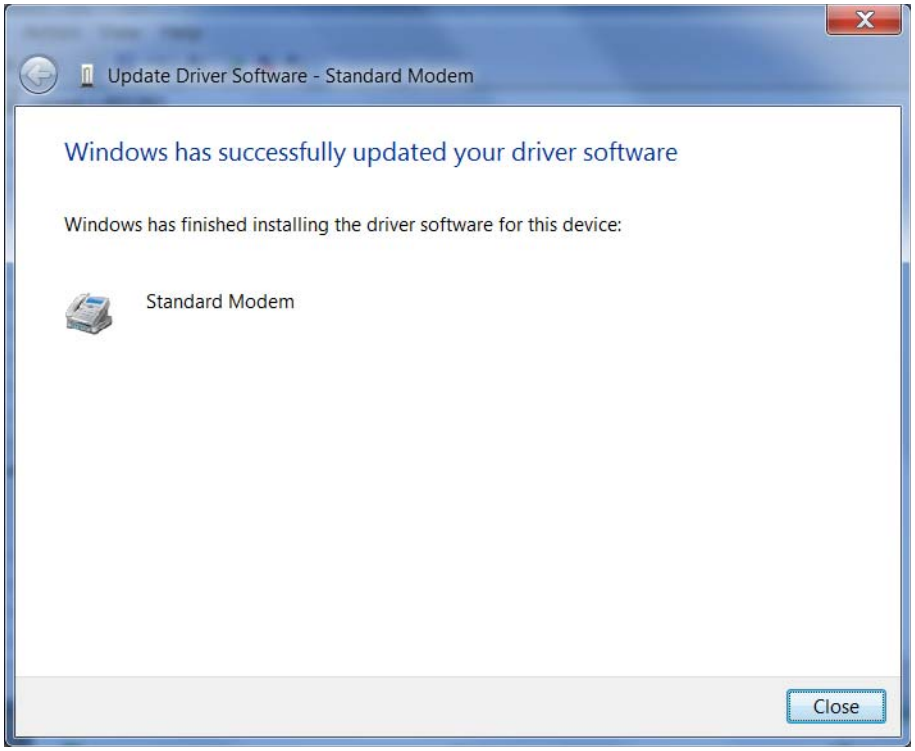

Update Driver Software - Standard Modem
Windows has successfully updated your driver software
Windows has finished installing the driver software for this device:
Standard Modem
Close

Figure A-15: Update Driver Software—Success

26. Click Close.

Creating a Dial-Up Networking (PPP) Connection

Once you have the driver for the modem installed on your computer, you can set up and configure Dial Up Networking (DUN) to use the modem as your connection to the Internet using PPP.

Note: No other device or program can use the COM port (serial port) configured for the modem driver while the DUN session is active.

Caution: *If you have an existing LAN connection, installing DUN for the modem may interfere with the LAN connection. We recommend disconnecting your LAN connection before using a PPP connection with your AirLink device.*

Once you have configured the DUN connection on your computer:

- The DUN connection may be set as the default connection for all network and Internet communication.
- The computer may be configured to dial the DUN connection when it cannot detect any network connection.

For instructions on changing these options, see Connection settings on page 285.

If you are using a DUN connection with any other network connection (such as Ethernet or Wi-Fi), you may need to use the route command in Windows to set up a static route through the device to access the location remotely over the PPP link and the cellular network. This guide does not provide information on the route command. Consult your network administrator for information on properly configuring routing.

Create a new network connection.

1. Select Start > Control Panel > Network and Sharing Center.

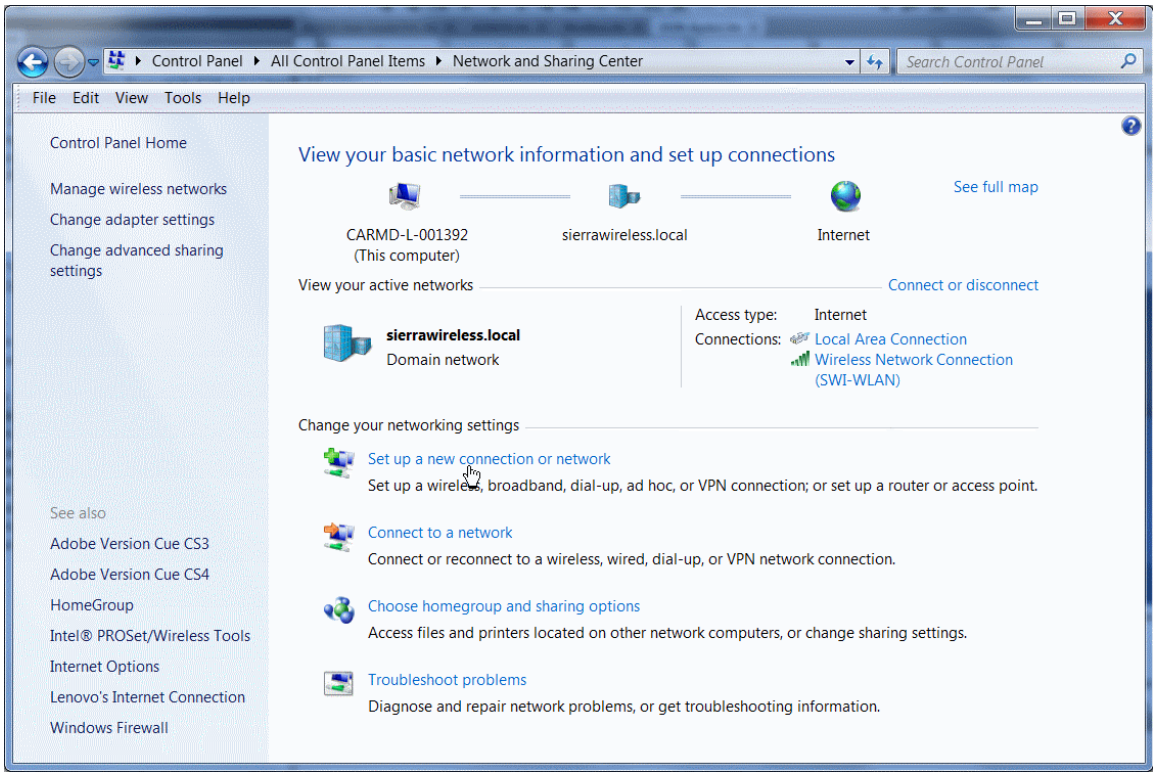

Control Panel ▸ All Control Panel Items ▸ Network and Sharing Center
Search Control Panel
File Edit View Tools Help
Control Panel Home
Manage wireless networks
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
CARMD-L-001392
(This computer)
sierrawireless.local
Internet
View your active networks
Connect or disconnect
sierrawireless.local
Domain network
Access type: Internet
Connections: Local Area Connection
Wireless Network Connection (SWI-WLAN)
Change your networking settings
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.
Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.
See also
Adobe Version Cue CS3
Adobe Version Cue CS4
HomeGroup
Intel® PROSet/Wireless Tools
Internet Options
Lenovo's Internet Connection
Windows Firewall

Figure A-16: Network and Sharing Center Window

2. Select Set up a new connection or network.

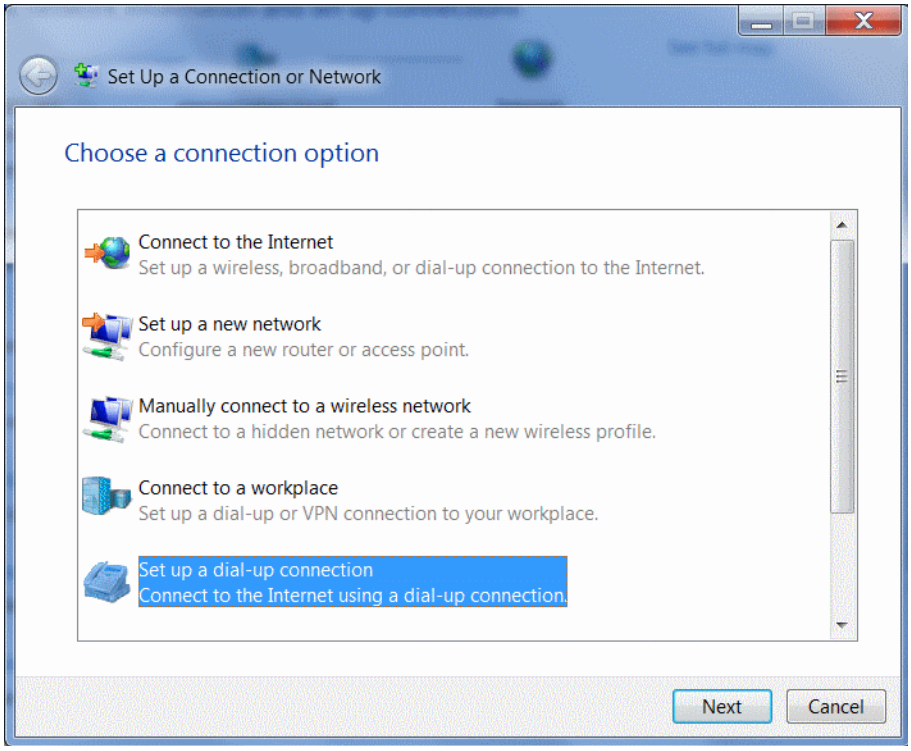

Set Up a Connection or Network
Choose a connection option
Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.
Set up a new network
Configure a new router or access point.
Manually connect to a wireless network
Connect to a hidden network or create a new wireless profile.
Connect to a workplace
Set up a dial-up or VPN connection to your workplace.
Set up a dial-up connection
Connect to the Internet using a dial-up connection.
Next
Cancel

Figure A-17: Set up a Connection or Network

3. Select Set up a dial-up connection.
4. Click Next.

   If you are asked which modem you want to use, select Standard 33600.

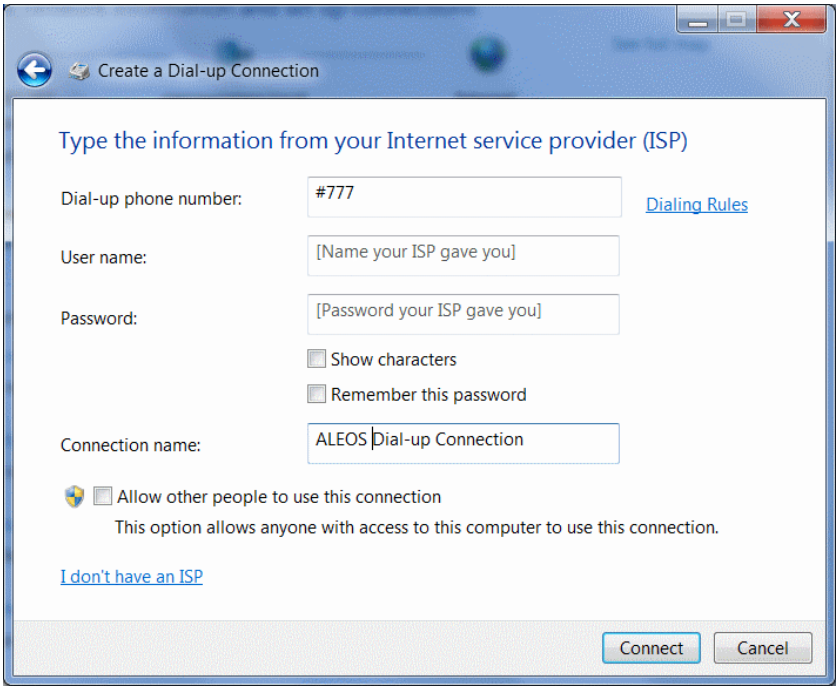


Figure A-18: Create a Dial up Connection

5. In the Dial-up phone number field, type “#777”.
6. Ignore the User name and Password fields.
7. In the Connection name field, type “ALEOS Dial-up Connection” or other desired name.
8. Click Connect.

   Alternatively, to connect to the ALEOS Dial-up network:

   a. Click the network connection icon[1] in the system tray.
   b. Select ALEOS Dial-up Connection.
   c. Click Connect.

Configure the DUN connection

After you complete the New Connection Wizard:

1. Click the network connection icon, select ALEOS Dial-up Connection, and click Connect.

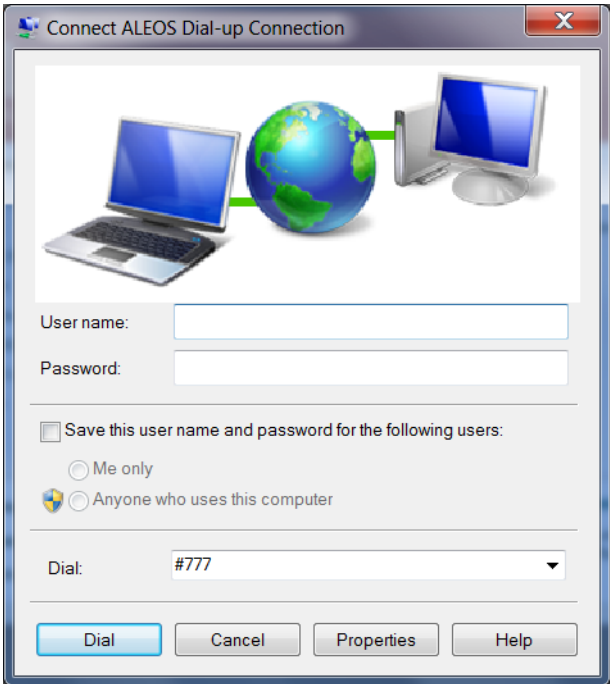


Figure A-19: DUN Connection

2. If you have a user name and password configured in ACEmanager for PPP connections, enter them in the User name and Password fields. Otherwise, leave these fields blank.
3. Click Properties.

1. The appearance of the connection icon varies depending on the type of connections available. For example, It may appear as , , or .

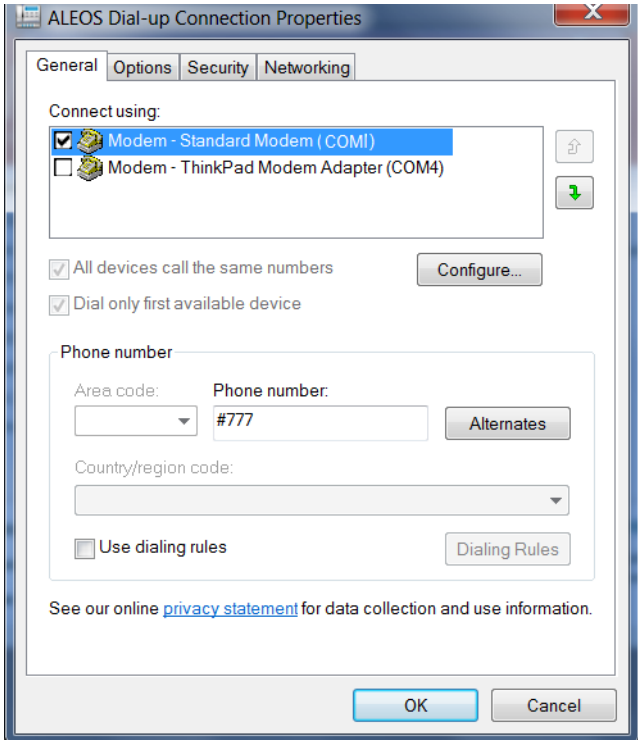


Figure A-20: DUN Properties

4. Confirm that the check box beside Use dialing rules is not selected.
5. Click Configure... (below the Connect using box).

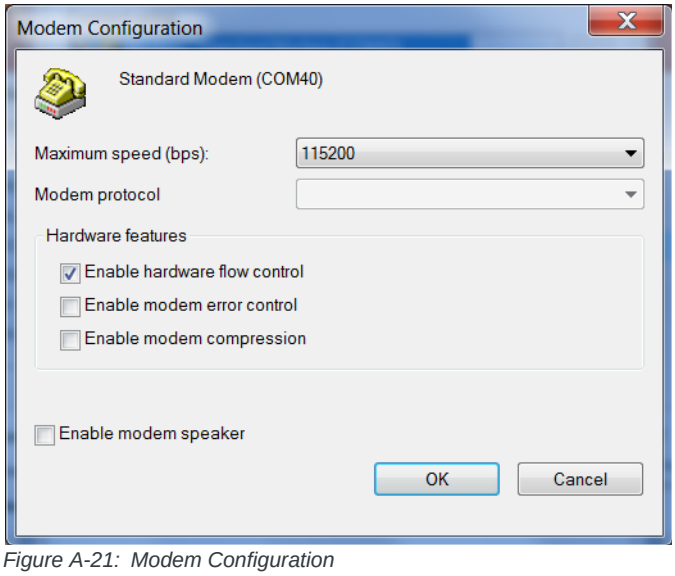


Figure A-21: Modem Configuration

6. Confirm that the Maximum speed (bps) is set to 115200.
7. Confirm that Enable hardware flow control is selected. Do not select any other options.
8. Click OK.

9. In the main properties window, select the Options tab.

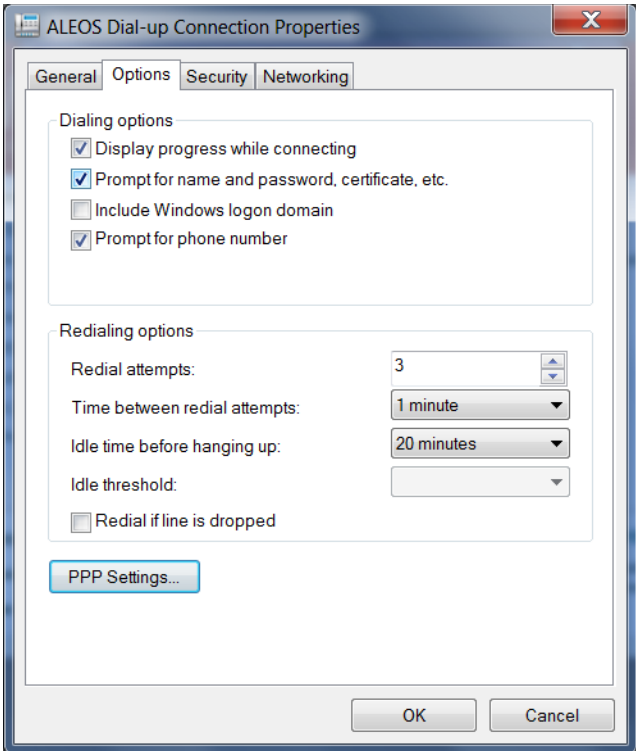


Figure A-22: Networking

10. Click PPP Settings.

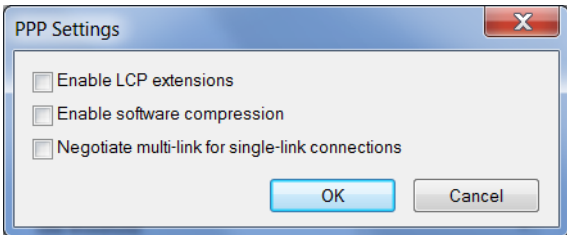


Figure A-23: PPP Settings

11. Clear the check boxes beside all three PPP settings.
12. Click OK.
13. Select the Networking tab.

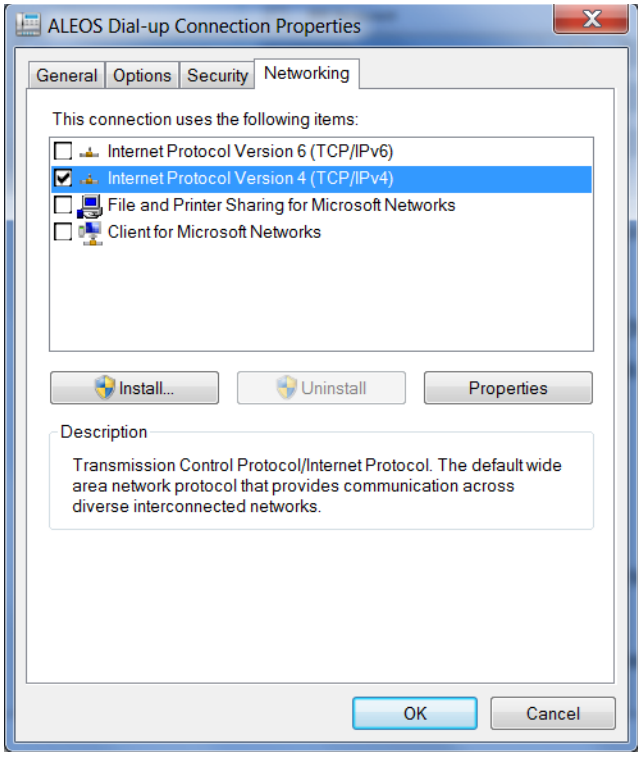


Figure A-24: DUN Connection > Networking tab

14. Select Internet Protocol Version 4 (TCP/IPv4) and then select Properties.

Tip: *For most configurations, getting the IP address and the DNS server address are automatic.*

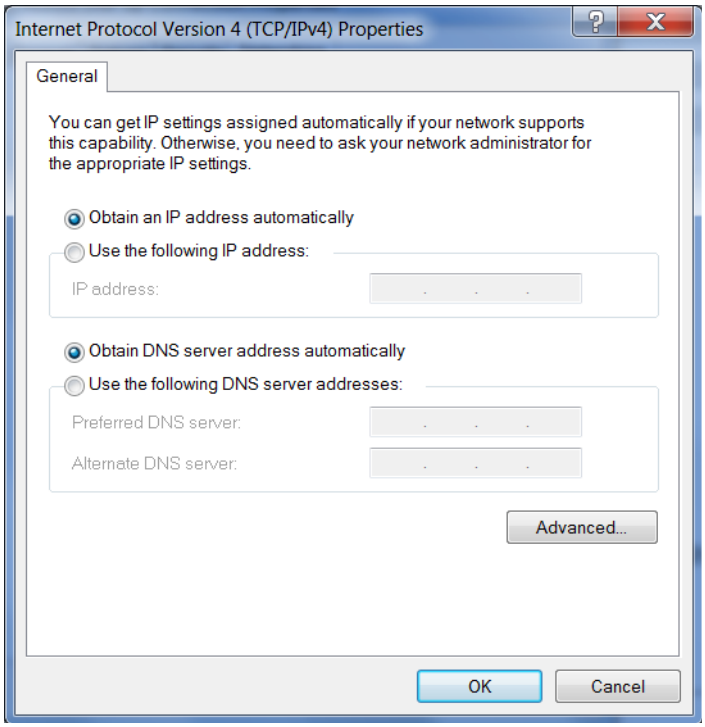

Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure A-25: TCP/IP Properties

15. Click Advanced.

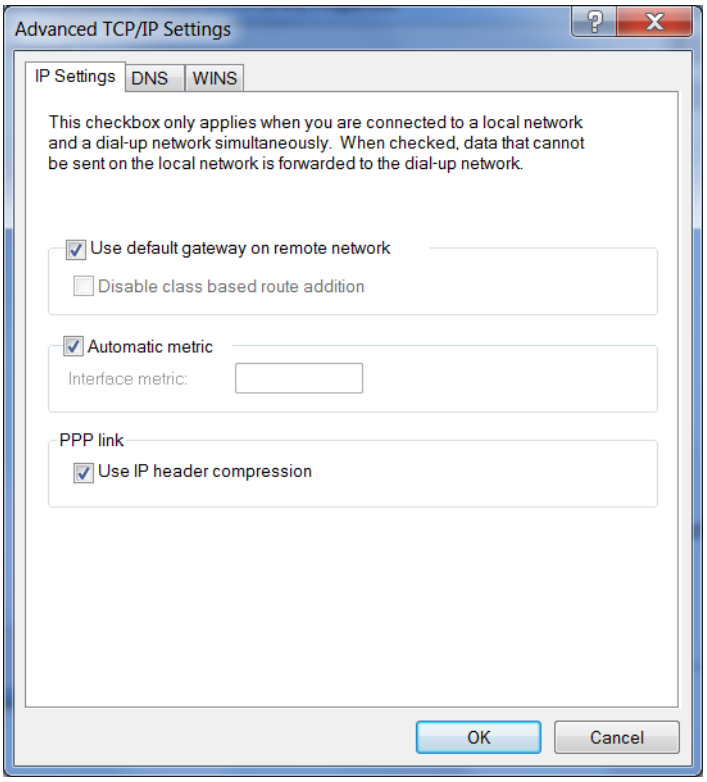

Advanced TCP/IP Settings
IP Settings
DNS
WINS
This checkbox only applies when you are connected to a local network and a dial-up network simultaneously. When checked, data that cannot be sent on the local network is forwarded to the dial-up network.
Use default gateway on remote network
Disable class based route addition
Automatic metric
Interface metric:
PPP link
Use IP header compression
OK
Cancel

Figure A-26: Advanced TCP/IP

16. Select Use default gateway on remote network.
17. Click OK.

Tip: *You may want to check the Options tab and change the settings for applications you use. The default options are generally applicable for most uses.*

Caution: *Unless specifically directed to do so by Support or your network administrator, you do not need to make any changes to the options on the Security tab.*

18. Click OK until you return to the Connect window.
19. Log in to ACEmanager and go to Serial > Port Configuration.

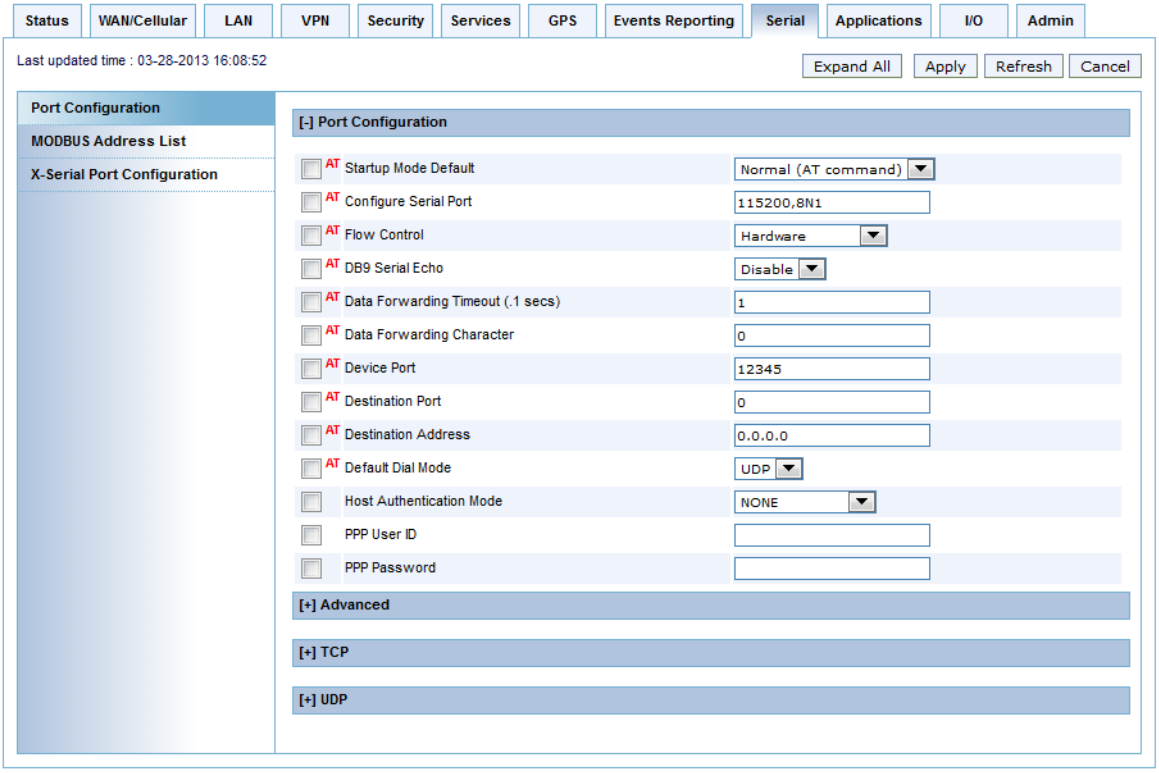


Figure A-27: ACEmanager: Serial > Port Configuration

20. Under Port Configuration:
    a. Set the Flow Control field to Hardware.
    b. Set the DB9 Serial Echo field to Disable.
21. Click Apply and reboot the device.

Connection settings

1. To set the default connection:
2. Go to Start > Control Panel > Network and Sharing Center.
3. Select Change adapter settings.

4. Right-click the icon for the DUN connection.

   If you want this to be your default connection, select Set as Default Connection.

   If it is already the default connection and you do not want it as your default connection, select Cancel as Default Connection.

If you do not want the DUN connection to be dialed when there is no other connection:

1. Go to Start > Control Panel > Internet Options.
2. Select the Connections tab.
3. Highlight the DUN connection and select Never dial a connection.
4. Click Apply.
5. Click OK.

Connecting to the Internet Using DUN

There are two methods you can use to connect the AirLink device to the Internet using DUN: ACEview, and the Windows DUN direct connection.

ACEview

ACEview is a utility which can maintain your DUN connection and monitor the connection of your AirLink device to the provider. If you have not already installed ACEview, obtain the most recent version from the Sierra Wireless AirLink website.

This guide assumes you have a default installation of ACEview.

1. Start ACEview.

   Go to Start > All Programs > Sierra Wireless > ACEview

2. Right-click the ACEview window to open the menu.

Figure A-28: ACEview: Menu

3. Select Settings.

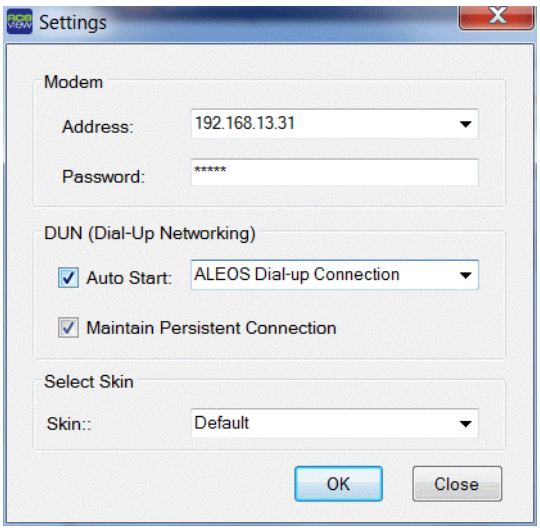


Figure A-29: ACEview: Connection Settings

4. Select Auto Start in the DUN section.
5. Select Maintain Persistent Connection.

   When selected, ACEview continually checks the DUN connection to ensure it is not down. If the connection is down, ACEview attempts to reconnect.

Tip: *When using the DUN connection, make sure the IP Address is set to the local IP address of the modem, i.e., 192.168.13.31 (by default).*

6. Click OK.

Windows DUN

You can directly use the Dial-up link for the DUN connection.

To start the DUN session:

1. Click the network connection icon (), select ALEOS Dial-up Connection, and click Connect.

   When you are connected, an icon should appear in the system tray showing the connection status.

Note: The speed shown in the connection is the speed between the modem and your computer. It is not the speed of the modem's connection to the provider or the Internet.

Caution: *For DUN connections on a Windows Mobility or other non-personal computer, the DNS settings may not be configured with the DUN connection. Go into the network settings and add DNS servers manually.*

B: Modbus/BSAP Configuration

B

The AirLink device supports Modbus ASCII, Modbus RTU, and BSAP, and can also emulate other protocols (like DF1) using the Modbus Variable feature.

Modbus Overview

The Modbus Protocol provides for client-server (i.e., master-slave) communications between intelligent devices. As a de facto standard, it is the most widely used network protocol in the industrial manufacturing environment to transfer discrete/analog I/O and register data between control devices. Modbus, BSAP, and other Modbus variations are often used in conjunction with telemetry devices.

Tip: *This section is just a brief overview of Modbus. For more information, refer to your Modbus equipment distributor or manufacturer or www.modbus.org.*

Telemetry

Telemetry is an automated communications process by which data is collected from instruments located at remote or inaccessible points and transmitted to receiving equipment for measurement, monitoring, display, and recording. Transmission of the information may be over physical pairs of wires, telecommunication circuits, radios, or satellites.

Remote Terminal Unit (RTU)

Modbus was originally designed to be used in a radio environment where packets were broadcast from a central station (i.e., master or host) to a group of remote units. Each remote unit, or Remote Terminal Unit (RTU), has a hexadecimal identification number (ID). The first part of the broadcast packet contains an RTU ID which corresponds to the ID of one of the remote units. The Modbus host looks for the ID and only sends to the unit with the matching ID; the RTU then replies back to the central station.

The RTU connects to such physical equipment as switches, pumps, and other devices, and monitors and controls these devices. The RTU can be part of a network set up for Supervisory Control and Data Acquisition.

Supervisory Control and Data Acquisition (SCADA)

Supervisory Control and Data Acquisition (SCADA) describes solutions across a large variety of industries and is used in industrial and engineering applications to monitor and control distributed systems from a master location. SCADA encompasses multiple RTUs, a central control room with a host computer (or network), and some sort of communication infrastructure.

SCADA allows for “supervisory” control of remote devices as well as acquiring data from the remote locations. Programmable Logic Controllers allow for a higher degree of automated SCADA.

Programmable Logic Controller (PLC)

A Programmable Logic Controller (PLC) is a small industrial computer which generally monitors several connected sensor inputs and controls attached devices (motor starters, solenoids, pilot lights/displays, speed drives, valves, etc.) according to a user-created program stored in its memory. Containing inputs and outputs similar to an RTU, PLCs are frequently used for typical relay control, sophisticated motion control, process control, Distributed Control System and complex networking.

Modbus TCP/IP

Modbus TCP/IP simply takes the Modbus instruction set and wraps TCP/IP around it. Since TCP/IP is the communications standard for the Internet and most networked computers, this provides a simpler installation. Modbus TCP/IP uses standard Ethernet equipment.

Modbus on UDP

When Sierra Wireless AirLink devices are used in place of radios, a AirLink device is connected to the central station (host) and an AirLink device is connected to each remote unit. When the AirLink device is configured for Modbus with UDP, the AirLink device connected to the host can store a list of IP addresses or names with matching IDs. When the host at the central station sends serial data as a poll request, the AirLink device at the host matches the RTU ID to a corresponding IP of a AirLink device at a remote unit. A UDP packet is assembled encapsulating the RTU ID and serial data transmitted from the host. The UDP packet is then transmitted to the specific AirLink device at the remote unit matching the RTU ID. The remote AirLink device then disassembles the packet before transmitting the RTU ID and serial data to the remote unit. The remote units operate in normal UDP mode and their data is sent to the host via the remote AirLink device and host AirLink device.

Configuring the AirLink Device at the Polling Host for Modbus on UDP

This section covers a Polling Host with standard Modbus, variations may need additional AT commands.

1. Configure the ports.

The destination port for the device at the host needs to match the device port (*DPORT) in use on all the modems at the remote sites. For example, if the remote device's device port (*DPORT) is "12345", then the Modbus host device's *S53* destination port should be set to "12345".

Take note of (or set) the Device Port setting in *DPORT to configure the destination port on the remote modems.

In ACEmanager, select *UDP* in the side menu. Select the appropriate *MD* mode from the drop down menu.

- **MD13**: Modbus ASCII
- **MD23**: Modbus RTU (Binary)
- **MD33**: BSAP
- **MD63**: Variable Modbus — individual parameters are set up manually.

If you do not have a static IP, the host device should be configured to report its current IP to a Dynamic DNS (DDNS) server with Dynamic DNS.

In the Host device's configuration, instead of an IP address for the Addr List (ATMLIST or ATMLISTX), substitute a single unique name for each device, i.e. remote1, remote2, etc.

When you configure Dynamic DNS for the host device, make note of your device name and domain setting in ACEmanager in the menu selection *Dynamic IP* to be used with the remote modems.

With names instead of IP addresses for the Address List, the host device queries the DNS server for the current IP address assigned to the specific name of a remote device to send a message corresponding to the ID.

When you use names instead of IP addresses, to ensure your modems are updated quickly with the correct IP addresses for the names, set the DNS settings as well. In ACEmanager, select *DNS*.

Configure *DNSUSER to the same IP address as the Dynamic DNS (*IPMANAGER1). If your modems have dynamic IP addresses and not static (the IP address can change when it is powered up), configure *DNSUPDATE to a low interval to allow frequent updates.

Configuring the Remote AirLink Devices for Modbus with UDP

This section covers standard Modbus settings for the AirLink device at the remote unit; variations may need additional commands.

1. Configure the ports

In ACEmanager, select Port Configuration in the side menu.

The destination port for the device at the host needs to match the device port in use on all the devices at the remote sites. For example, if the remote device's device port (see below) is "12345", then the Modbus host device's *S53* destination port should be set to "12345".

Set the destination port (S53) to match the device port of the host device (*DPORT). Make sure the device port of the remote device (*DPORT) matches the destination port of the host device (S53).

Configure IP Addresses for the Host

If the Host device has a static IP address, enter it in the Destination Address for S53.

Note: With a name instead of IPs for the host device, the remote devices query the DNS server for the current IP assigned to the host device before sending data back to the host.

If the device at the host has a dynamic IP and is using Dynamic DNS, instead of an IP address for S53, specify the name of the host device (**). If the remote devices are using a different DDNS than the host device, you need to specify the fully qualified domain name (**+*DOMAIN).

*Note: Setting the Host device IP address as the S53 Destination Address provides a low level security. The device does not forward UDP traffic unless the source IP/port matches what is in S53. However, if you set *AIP=1, the device forwards UDP traffic from any source IP address as long as it is accessing the device on the configured *DPORT.*

1. Configure the default mode for start-up.

Each device at the remote locations needs to be configured to communicate with the device at the host. In ACEmanager, select *UDP* in the side menu.

   a. Enable *S82*, UDP auto answer.
   b. Set *S83* to the idle time-out applicable to your application, commonly 20.

2. Configure other RTU settings.

Other parameters may need to be changed, but this is dependent on the RTU type being used. At a minimum, this typically involves setting the proper serial settings to match your RTU.

3. Optional: Dynamic IP Address

If you do not have a static IP, the host device should be configured to report its current IP to a Dynamic DNS (DDNS) server with Dynamic DNS.

Match the name of the device to the names specified in the host device's MLIST or MLISTX for the connected RTU.

When you configure Dynamic DNS for the host device, note your device name and domain setting in ACEmanager in the menu selection *Dynamic IP* to be used with the remote devices.

When you use names instead of IP addresses, to ensure your devices are updated quickly with the correct IP addresses for the names, set the DNS settings as well.

Configure *DNSUSER to the same IP address as the Dynamic DNS (*IPMANAGER1). If your devices have dynamic IP addresses and not static (the IP address can change when it is powered up), configure *DNSUPDATE to a low interval to allow frequent updates.

C: SNMP: Simple Network Management Protocol

C

Management Information Base (MIB)

ALEOS includes a Management Information Base (MIB) that contains information specific to the AirLink device. Reports based on this database are sent in a form designed to be parsed by the NMS. The data is hierarchical with entries addressed through object identifiers.

The MIB complies with:

- RFC 1213 and MIB-II
- RFC 2665 — Ethernet-Like Interface Types
- RFC 2863 — The Interfaces Group MIB

SNMP Traps

SNMP traps are alerts that can be sent from the managed device to the Network Management System when an event happens. Your AirLink device is capable of sending traps when the network connection becomes available.

To send SNMP traps:

1. In ACEmanager, go to Services > Management (SNMP).
2. Configure the fields under Trap Server User. (For more information, see Management (SNMP) on page 177.)
3. Go to Events Reporting > Actions.
4. In the Action Type field select SNMP trap. (For more information, see Action Type on page 213.)
5. Go Events Reporting > Events and configure monitoring for the event type that will trigger the SNMP trap. For example, the event type could be RSSI, thresholds, network state, hardware temperature, etc.

Sierra Wireless MIB

This section show the contents of the Sierra Wireless MIB file. When this file is loaded onto a remote SNMP client, you can query the Sierra Wireless specific objects listed in this file.

For a text copy of this MIB file, go to www.sierrawireless.com/en/Support/Downloads.aspx, and select your AirLink device.

```
SIERRA-MIB DEFINITIONS ::= BEGIN

IMPORTS
   OBJECT-TYPE, NOTIFICATION-TYPE, MODULE-IDENTITY, IpAddress,
   Integer32, Opaque, enterprises, Counter32, Unsigned32
      FROM SNMPv2-SMI

   TEXTUAL-CONVENTION, DisplayString, TruthValue
FROM SNMPv2-TC;

sierrawireless MODULE-IDENTITY
   LAST-UPDATED "201202290000Z"
   ORGANIZATION "Sierra Wireless Inc"
   CONTACT-INFO
"Sierra Wirelss Inc
      "

   DESCRIPTION
""
   REVISION "201202290000Z"

   DESCRIPTION
"This file defines the private Sierra MIB extensions."

   ::= { enterprises 20542 }

sharks OBJECT IDENTIFIER ::= { sierrawireless  9}

-- MIB versions

mibversion1 OBJECT IDENTIFIER ::= { sharks  1}

--  GUI Tabs for Sharks

statustab OBJECT IDENTIFIER ::= { mibversion1  1}
cellulartab OBJECT IDENTIFIER ::= { mibversion1  2}
lantab OBJECT IDENTIFIER ::= { mibversion1  3}
vpntab OBJECT IDENTIFIER ::= { mibversion1 4}
securitytab OBJECT IDENTIFIER ::= { mibversion1  5}
servicestab OBJECT IDENTIFIER ::= { mibversion1  6}
gpstab OBJECT IDENTIFIER ::= { mibversion1  7}
eventsreportingtab OBJECT IDENTIFIER ::= { mibversion1  8}
serialtab OBJECT IDENTIFIER ::= { mibversion1  9}
iotab OBJECT IDENTIFIER ::= { mibversion1  10}
admintab OBJECT IDENTIFIER ::= { mibversion1  11}
snmpconfig OBJECT IDENTIFIER ::= { mibversion1  12}

--  status elements

home   OBJECT IDENTIFIER ::= { statustab  1}
cellular OBJECT IDENTIFIER ::= { statustab  2}
lan  OBJECT IDENTIFIER ::= { statustab  3}
```

```
vpn    OBJECT IDENTIFIER ::= { statustab  4}
security    OBJECT IDENTIFIER ::= { statustab  5}
services    OBJECT IDENTIFIER ::= { statustab  6}
gps    OBJECT IDENTIFIER ::= { statustab  7}
serial    OBJECT IDENTIFIER ::= { statustab  8}
about    OBJECT IDENTIFIER ::= { statustab  9}


-- home status elements

phoneNumber OBJECT-TYPE
SYNTAX DisplayString (SIZE (10))
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 17 }

ipAddress OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 301 }

networkState OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 259 }

rssi OBJECT-TYPE
SYNTAX INTEGER(-125..-50)
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 261 }

gprsnetworkOperator OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 770 }

cdmanetworkOperator OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 644 }
```

```
gprsECIO OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
 DESCRIPTION ""
::= { home 772 }

cdmaECIO OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
  DESCRIPTION ""
::= { home 643 }

powerIn OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 266 }

boardTemprature OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 267 }

networkServiceType OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 264}

aleosSWVer OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 4 }

netChannel OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 260 }

cellularBytesSent OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
```

```
STATUS current
   DESCRIPTION ""
::= { home 283 }

cellularBytesRecvd OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 284 }


deviceName OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 1154 }

-- cellular status elements

wanIP OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 301 }

electronicID OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 10 }

iccid OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 771 }

cellid OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 773 }

lac OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
```

```
STATUS current
   DESCRIPTION ""
::= { cellular 774 }

imsi OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 785 }

keepAliveIpAddress OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 1105 }

keepAlivePingTime OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 1104 }

dnsServer1 OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 1082 }

dnsServer2 OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 1083 }

cellBand OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 2056 }

apn OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 2151 }
```

```
wanUseTime OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 5046 }

rscp OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 10249 }

errorRate OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 263 }

bytesSent OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 283 }

bytesRecvd OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 284 }

packetsSent OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 281 }

packetsRecvd OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 282 }

prlVersion OBJECT-TYPE
SYNTAX INTEGER
```

```
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 642 }

prlUpdateStatus OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 646 }

sid OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 648 }

nid OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 649 }

pnOffset OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 650 }

baseClass OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 651 }

-- LAN status elements

usbMode OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { lan 1130 }

vrrpEnabled OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
```

```
STATUS current
   DESCRIPTION ""
::= { lan 9001 }

lanpacketsSent OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { lan 279 }

lanpacketsRecvd OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { lan 280 }

wifipacketsSent OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { lan 10405 }

wifipacketsRecvd OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { lan 10406 }

wifiBridgeEnabled OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { lan 10401 }

wifiSecurityType OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { lan 4509 }

wifiAPStatus OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { lan 4506 }
```

```
wifiSSID OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { lan 4507 }

wifiChannel OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { lan 4508 }

-- VPN status elements


incomingOOB OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { vpn 3177 }

outgoingOOB OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { vpn 3178 }

outgoingHostOOB OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { vpn 3179 }


vpn1Status OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { vpn 3176 }

vpn2Status OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
```

```
::= { vpn 3205 }

vpn3Status OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { vpn 3231 }

vpn4Status OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { vpn 3257 }

vpn5Status OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { vpn 3283 }

-- Security status elements

dmz OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { security 5113 }

portForwarding OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { security 5112 }

portFilteringIn OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { security 3505 }

portFilteringOut OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { security 3506 }
```

```
trustedHosts OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { security 1062 }

macFiltering OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { security 3509 }

badPasswdCount OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { security 385 }

ipRejectCount OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { security 386 }

ipRejectLog OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { security 387 }

-- Services status elements

aceNet OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { services 5026 }

aceManager OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { services 1149 }
```

```
dynamicDnsService OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { services 5011 }

fullDomainName OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { services 5007 }

-- GPS status elements

gpsFix OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { gps 900 }

satelliteCount OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { gps 901 }

latitude OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { gps 902 }

longitude OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { gps 903 }

heading OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { gps 904 }

speed OBJECT-TYPE
```

```
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { gps 905 }

engineHours OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { gps 906 }

-- Serial status elements

serialPortMode OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { serial 1043 }

tcpAutoAnswer OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { serial 1048 }

udpAutoAnswer OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { serial 1054 }

serialPacketsSent OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { serial 273 }

serialPacketsRecvd OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { serial 274 }

-- About status elements
```

```
deviceModel OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { about 7 }


radioModelType OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { about 9 }

radioFirmwareVersion OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { about 8 }

deviceID OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { about 25 }

macAddress OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { about 66 }

aleosSWVersion OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { about 4 }

deviceHwConfiguration OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { about 5 }

msciVersion OBJECT-TYPE
SYNTAX DisplayString
```

```
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { about 3 }

-- Read Write values

snmpenable OBJECT-TYPE
SYNTAX INTEGER {
       disabled(0),
       enabled(1)}
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 10040 }

snmpversion OBJECT-TYPE
SYNTAX INTEGER {
       snmpv2c(2),
       snmpv3(3)}
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10041 }

snmpport OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10042 }

snmpContact OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  2730 }

snmpName OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  2731 }

snmpLocation OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  2732 }
```

```
rocommunity OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10063 }

rouser OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10045 }

rosecuritylvl OBJECT-TYPE
SYNTAX INTEGER {
       noauthnopriv(0),
       authnopriv(1),
       authpriv(2)}
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10046 }

roauthtype OBJECT-TYPE
SYNTAX INTEGER {
       md5(0),
       sha(1) }
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10047 }

roauthkey OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10048 }

roprivtype OBJECT-TYPE
SYNTAX INTEGER {
       aes(0),
       des(1) }
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10049 }

roprivkey OBJECT-TYPE
SYNTAX DisplayString
```

```
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 10050 }


rwcommunity OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 10064 }

rwuser OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 10051 }

rwsecuritylvl OBJECT-TYPE
SYNTAX INTEGER {
       noauthnopriv(0),
       authnopriv(1),
       authpriv(2)}
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 10052 }

rwauthtype OBJECT-TYPE
SYNTAX INTEGER {
       md5(0),
       sha(1) }
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 10053 }

rwauthkey OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 10054 }


rwprivtype OBJECT-TYPE
SYNTAX INTEGER {
       aes(0),
       des(1) }
MAX-ACCESS read-write
```

```
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10055 }

rwprivkey OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10056 }


trapipAddress OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 1166 }

trapport OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10043 }

engineid OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10044 }

trapcommunity OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10065 }

trapuser OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10057 }

trapsecuritylvl OBJECT-TYPE
SYNTAX INTEGER {
       noauthnopriv(0),
       authnopriv(1),
       authpriv(2)}
```

```
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 10058 }

trapauthtype OBJECT-TYPE
SYNTAX INTEGER {
       md5(0),
       sha(1) }
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 10059 }

trapauthkey OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 10060 }


trapprivtype OBJECT-TYPE
SYNTAX INTEGER {
       aes(0),
       des(1) }
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 10061 }

trapprivkey OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 10062 }


rebootmodem OBJECT-TYPE
SYNTAX INTEGER {
       nop(0),
       reboot(1) }
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 65001 }



-- Notifications starting at 1000
```

```
modemNotifications OBJECT IDENTIFIER ::= { mibversion1  1000 }


value OBJECT-TYPE
   SYNTAX      DisplayString
   MAX-ACCESS  accessible-for-notify
   STATUS      current
   DESCRIPTION
      "value of MSCIID that triggered this event"
::= { modemNotifications 500 }

digitalInput1 NOTIFICATION-TYPE
   OBJECTS     { value }
   STATUS      current
   DESCRIPTION
      "Digital Input 1 MSCIID 851"
::= { modemNotifications 1 }


digitalInput2 NOTIFICATION-TYPE
   OBJECTS     { value }
   STATUS      current
   DESCRIPTION
      "Digital Input 1 MSCIID 852"
::= { modemNotifications 2 }

digitalInput3 NOTIFICATION-TYPE
   OBJECTS     { value }
   STATUS      current
   DESCRIPTION
      "Digital Input 1 MSCIID 853"
::= { modemNotifications 3 }

digitalInput4 NOTIFICATION-TYPE
   OBJECTS     { value }
   STATUS      current
   DESCRIPTION
      "Digital Input 1 MSCIID 854"
::= { modemNotifications 4 }

pulseAccumulator1 NOTIFICATION-TYPE
   OBJECTS     { value }
   STATUS      current
   DESCRIPTION
      "Pulse Accumulator 1 MSCIID 4002"
::= { modemNotifications 5 }


pulseAccumulator2 NOTIFICATION-TYPE
   OBJECTS     { value }
   STATUS      current
   DESCRIPTION
```

```
        "Pulse Accumulator 2 MSCIID 4003"
::= { modemNotifications 6 }

pulseAccumulator3 NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Pulse Accumulator 3 MSCIID 4004"
::= { modemNotifications 7 }

pulseAccumulator4 NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Pulse Accumulator 1 MSCIID 4005"
::= { modemNotifications 8 }

analogInput1 NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Analog  Input 1 MSCIID 855"
::= { modemNotifications 9 }


analogInput2 NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Analog  Input 2 MSCIID 856"
::= { modemNotifications 10 }

analogInput3 NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Analog  Input 3 MSCIID 857"
::= { modemNotifications 11 }

analogInput4 NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Analog  Input 4 MSCIID 858"
::= { modemNotifications 12 }

scaledAnalogInput1 NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Scaled Analog  Input 1 MSCIID 4041"
::= { modemNotifications 13 }
```

```
scaledAnalogInput2 NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Scaled Analog  Input 2 MSCIID 4042"
::= { modemNotifications 14 }

scaledAnalogInput3 NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Scaled Analog  Input 3 MSCIID 4043"
::= { modemNotifications 15 }

scaledAnalogInput4 NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Scaled Analog  Input 4 MSCIID 4044"
::= { modemNotifications 16 }

gpsFixNotification NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "GPS Fix MSCIID 900"
::= { modemNotifications 17 }

vehicleSpeed NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Vehicle Speed MSCIID 905"
::= { modemNotifications 18 }

engineHoursNotification NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Engine Hours MSCIID 906"
::= { modemNotifications 19 }

headingChange NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Heading Change MSCIID 904"
::= { modemNotifications 20 }

rssiNotification NOTIFICATION-TYPE
```

```
    OBJECTS    { value }
    STATUS     current
    DESCRIPTION
       "RSSI MSCIID 261"
::= { modemNotifications 21 }

networkStateNotification NOTIFICATION-TYPE
    OBJECTS    { value }
    STATUS     current
    DESCRIPTION
       "Network State MSCIID 259"
::= { modemNotifications 22 }

networkService NOTIFICATION-TYPE
    OBJECTS    { value }
    STATUS     current
    DESCRIPTION
       "Network Service 264"
::= { modemNotifications 23 }

networkErrorRate NOTIFICATION-TYPE
    OBJECTS    { value }
    STATUS     current
    DESCRIPTION
       "Network Error Rate MSCIID 263"
::= { modemNotifications 24 }

periodicReports NOTIFICATION-TYPE
    OBJECTS    { value }
    STATUS     current
    DESCRIPTION
       "Periodic Reports MSCIID 270"
::= { modemNotifications 25 }

powerInNotification NOTIFICATION-TYPE
    OBJECTS    { value }
    STATUS     current
    DESCRIPTION
       "Power In  MSCIID 266"
::= { modemNotifications 26 }

boardTemp NOTIFICATION-TYPE
    OBJECTS    { value }
    STATUS     current
    DESCRIPTION
       "Board Temperature MSCIID 267"
::= { modemNotifications 27 }

cdmaTemp NOTIFICATION-TYPE
    OBJECTS    { value }
    STATUS     current
    DESCRIPTION
```

```
      "CDMA Temperature MSCIID 641"
::= { modemNotifications 28 }


dailyDataUsage NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Daily Data Usage MSCIID 25001"
::= { modemNotifications 29 }

monthlyDataUsage NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Monthly Data Usage MSCIID 25002"
::= { modemNotifications 30 }

END
```

D: AT Commands

AT Command Set Summary

Using a terminal connection (Telnet) or SSH protocol, you can send AT commands to configure the device, command it to do something, or query a setting.

- AT commands must always be terminated by a carriage return <CR> (ASCII character 0x0D), i.e., pressing enter on the keyboard. Some may also include a new line or line feed <LF>.
- If **E=1** (Echo On), the AT command (including the terminating <carriage return>) is displayed (output) before any responses.
- Two settings affect the format of AT command output: V (Verbose) and Q (Quiet).
- If Q=1 (Quiet On), no result codes are output whatsoever, so there is no response generated by a (non-query) command.
- If Q=0 (Quiet Off), result codes are output. The format of this output is then affected by the Verbose setting.

  If Quiet mode is off, the result code is affected as follows:

  For V=1 (Verbose mode), the textual result code is surrounded by a carriage return and new line. Any AT query response is also surrounded by a carriage return and new line.

  For V=0 (Terse mode), a numeric result code is output with a single trailing carriage return (no new line is output), while any AT query response is followed by a carriage return and new line (there is no preceding output).
- For example, possible output to the AT command “AT” with carriage return (assuming quiet mode is not on) is:

  carriage return — if V=0

  carriage return and new line OK another carriage return and new line — if V=1

Note: AT commands work for the port on which they are executed. For example, if the user types ATE1 and then AT&W using a USB/serial port connection, it sets the USB/serial port to Echo On but not the telnet connection or the RS232 serial port.

If you need to change the port for Telnet (for example, you have the default port blocked on your firewall), the option is on the Services > Telnet/SSH tab. The default Telnet port is 2332. You can also change the Telnet timeout; if the connection is idle, default timeout is 2 minutes. This is the internal Telnet on the device to pass AT commands and not TCP PAD.

AT commands are shown in upper case, but they are not case sensitive.

This appendix organizes the commands into functional groups to allow you to more quickly locate a desired command when you know the operation but not the command. Commands under each topic are listed alphabetically.

Note: Some of the configuration commands listed here are only available as AT commands.

Reference Tables

Result codes are not shown in the command tables unless special conditions apply. Generally the result code OK is returned when the command has been executed. ERROR may be returned if parameters are out of range, and is returned if the command is not recognized or is not permitted in the current state or condition of the AirLink device.

AT command topics in this appendix:

- Standard (Hayes) commands on page 366
- Device Updates on page 323
- Status on page 323
- WAN/Cellular on page 328
- LAN on page 334
- Wi-Fi on page 336
- VPN on page 339
- Security on page 344
- Services on page 345
- GPS on page 353
- Serial on page 359
- I/O on page 371
- Applications on page 372
- Admin on page 373

Device Updates

Table D-1: Device Update AT Commands

Command	Description
***TPLUPDATE**	This AT command updates templates (configuration files) remotely. The template files must be accessible on an FTP server. The command parameters are: AT*TPLUPDATE=Server_IP,USER_NAME,PASSWORD,FILE_NAME where: • SERVER_IP is the IP address of the FTP server. • USER_NAME is the user name used to access the FTP server. • PASSWORD is the password used to access the FTP server. • FILE_NAME is the name of the template file on the FTP server that you want to apply to the AirLink device. The must be stored on the FTP User_Name home, not in a sub-folder. Example: AT*TPLUPDATE=192.168.17.111,MyUserName,MyPassword,NewTemplate.xml When the template is successfully applied, the message displayed is: `Template applied successfully` OK

Status

Table D-2: Status AT Commands

Command	Description
***BAND?**	HSPA and LTE fallback to HSPA only. Query the current radio module band.
***CELLINFO?**	Query cellular connection information.
***CELLINFO2?**	Query in depth cell information.
+CIMI?	HSPA and LTE only. Query the IMSI.
***DEVICEID?**	When the device is configured to use the device ID with GPS reports, this command displays the 64-bit device ID created from the ESN/IMEI or phone. *Note: If the device is not configured to use the device ID with GPS reports, the command returns "NOT SET".*
***DNS1?** ***DNS2?**	Query the primary DNS (*DNS1) and secondary (*DNS2) IP addresses. AT*DNS1? to query DNS1 AT*DNS2? to query DNS2
+ECIO?	Query the signal quality.

Table D-2: Status AT Commands (Continued)

Command	Description
***ETHMAC?**	Query the MAC address of the Ethernet port • AT*ETHMAC? — Returns the MAC address of the main Ethernet port If you have a GX Series device with a Dual Ethernet X-Card installed: • AT*ETHMAC?2 — Returns the MAC address of the Ethernet X-Card port marked eth2 • AT*ETHMAC?3 — Returns the MAC address of the Ethernet X-Card port marked eth3
***ETHSTATE?**	Query the connection state (speed and duplex) of the Ethernet port. • AT*ETHSTATE? — Returns the speed and duplex state of the main Ethernet port (e.g. 100Mb/s Full Duplex) If you have a GX Series device with a Dual Ethernet X-Card installed: • AT*ETHSTATE2? — Returns the speed and duplex state of the Ethernet X-Card port marked eth2 • AT*ETHSTATE3? — Returns the speed and duplex state of the Ethernet X-Card port marked eth3
***GLOBALID?**	Query the global ID used by AVMS to identify the device.
***HOSTCOMMLVL?**	Query the serial host signal level. Response example: DCD:LOW; DTR:LOW; DSR:HIGH; CTS:HIGH; RTS:LOW
+HWTEMP?	Query the internal temperature of the radio module (in degrees Celsius).
I[n]	Query device information. • n omitted—device model • n=0—device model • n=1—ALEOS software version, hardware revision, boot version • n=2—Radio module firmware version • n=3—Radio module's unique ID (ESN, IMIEI, or EID)
+ICCID?	HSPA and LTE only. Query the SIM ID.
***LTERSRQ?**	LTE only Query the LTE signal quality (in dB). For more information, see LTE Signal Quality (RSRQ) on page 45.
***LTERSRP?**	LTE only Query the LTE signal strength (in dBm). For more information, see LTE Signal Strength (RSRP) on page 44.
***NETCHAN?**	Query the current cellular network channel.

Table D-2: Status AT Commands (Continued)

Command	Description
NETIP?	Query the current WAN IP address of the device reported by the internal module (generally obtained from your Mobile Network Operator). If the device is connected in Wi-Fi Client mode, the Wi-Fi IP address is returned. If you have an Internet-routable IP address, you can use this address to contact devices from the Internet. If your device uses a different WAN (such as a Wi-Fi client) or is on a private cellular network, you can use this address to contact the device from another host on the same WAN network. If required, use AT**NETALLOWZEROIP to allow displaying an IP address ending in a zero. *Note: If there is no current network IP address, 0.0.0.0 is returned.*
***NETOP?**	Query the Mobile Network Operator of the active connection. If you are roaming, the roaming operator is returned, if the home operator allows this.
***NETPHONE?**	Query the device's cellular phone number, if applicable or obtainable.
***NETRSSI?**	Query the current RSSI (Receive Signal Strength Indicator) for non-LTE cellular connections, as a negative dBm value.
***NETSERV?**	Query the current connection type (e.g., LTE, HSPA+, EV-DO Rev A, etc.).
***NETSERVICE_RAW?**	Query the numeric value for the network service type. • 8—2G (1x, EDGE, GPRS) • 10—2G roaming • 16—3G (EV-DO Rev. A, HSPA, HSPA+, UMTS) • 18—3G roaming • 64—4G

Table D-2: Status AT Commands (Continued)

Command	Description
***NETSTATE?**	Query the network state of the current WAN connection. AT*NETSTATE? returns: • Connecting To Network—The device is in the process of trying to connect to the cellular network. • Network Authentication Fail—Authentication to the cellular network has failed. Verify settings to activate the device. • Data Connection Failed—The device failed to connect, and it is now waiting a set time interval before it attempts to reconnect. Verify settings to activate the device. • Network Negotiation Fail—Network connection negotiation failed. This is usually temporary and often clears up during a subsequent attempt. • Network Ready—The device is connected to the 1x cellular network and ready to send data. • Network Ready - Wi-Fi—Device is connected to a Wi-Fi network in client mode. • Network Dormant—The device is connected to the 1x cellular network, but the link is dormant. It will be woken up when data is sent or received. • No Service—There is no cellular network detected. • Hardware Reset—The internal module is being reset. This is a temporary state. • No SIM or Unexpected SIM status—No SIM, SIM installed incorrectly, or another SIM error. • Awaiting Provisioning—EV-DO device without an account and hasn't had an account or the provisioning has been erased from the radio. • Provisioning... —An EV-DO device in the process of writing the account data to the radio. • Not Connected-Waiting for Activity — “Always On Connection” has been disabled and the device is waiting for outgoing traffic to mount the PDP context. • Not Connected-Radio Connect off—the RADIO_CONNECT AT command was entered, and the PDP context is manually disabled. • SIM Locked, but bad SIM PIN. • SIM PIN incorrect 3 attempts left. • SIM PIN incorrect 2 attempts left. • SIM PIN incorrect 1 attempts left. • SIM PIN incorrect 0 attempts left. • SIM Blocked, Bad unlock code. • SIM Blocked, unblock code incorrect.

Table D-2: Status AT Commands (Continued)

Command	Description
***NETSTATE_RAW?**	Query numeric value of the network state of the current WAN connection: • 1—Connecting To Network—The device is in the process of trying to connect to the cellular network. • 4—Network Access Denied—Connection rejected. • 5—Network Ready—WAN is using cellular and is online. • 7—No Service—The WAN link is down or unavailable • 9—No SIM or Unexpected SIM status—No SIM, SIM installed incorrectly, or another SIM error. • 11—Awaiting Provisioning—EV-DO device without an account and hasn't had an account or the provisioning has been erased from the radio. • 12—Data Connection Failed - Waiting to Retry—The device failed to connect, and it is waiting a set time interval before it attempts to reconnect. Or • 12—Provisioning... —An EV-DO device in the process of writing the account data to the radio. • 13—SIM Locked, but bad SIM PIN. • 14—SIM PIN incorrect 3 attempts left. • 15—SIM PIN incorrect 2 attempts left. • 16—SIM PIN incorrect 1 attempts left. • 17—SIM PIN incorrect 0 attempts left. • 18—SIM Blocked, Bad unlock code. • 19—SIM Blocked, unblock code incorrect. • 27—Network Ready - Wi-Fi—WAN is using WiFi Client and is connected. • 30—Not Connected-Waiting for Activity — "Always On Connection" has been disabled and the device is waiting for outgoing traffic to mount the PDP context. • 31—Not Connected-Radio Connect off—the RADIO_CONNECT AT command was entered, and the PDP context is manually disabled.
+PRL?	CDMA and LTE fallback to EV-DO only Query CDMA Preferred Roaming List (PRL) version.
***PRLSTATUS?**	CDMA only Query the status of the most recent PRL update • n=0—None (No update) • n=1—In progress • n=2—Update successful The return of any other value indicates that the update failed.
***USBNETSTATE?**	Query the status of the USB connection. AT*USBNETSTATE? returns: • None—There are no USB connections to the AirLink device. • 8 MB/s Half Duplex—There is a USB connection to the device.

WAN/Cellular

A reboot is required before the WAN/Cellular AT Commands described in the following table take effect.

Table D-3: WAN/Cellular AT Commands

Command	Description
***AUTOPRL**	CDMA only. Query or set automatic Preferred Roaming List updates AT*PRL? to query AT*PRL=n to set • n=0—Disable • n=1—Enable *Note: To query the current PRL, use +PRL?.*
***AUTOPRLFREQ**	CDMA only. Query or set how often the PRL automatically updates. AT*AUTOPRLFREQ? to query AT*AUTOPRLFREQ=n to set • n= interval to check for updates (in days)
!BAND	HSPA and LTE fallback to HSPA only. Query or set the RF band range or technology. AT!BAND? to query a value sent since the device was last rebooted. AT!BAND=hh to set at the next reboot. • hh=00—All bands • hh=03—GSM 900/1800 • hh=05—GSM All • hh=08—WCDMA All • hh=10—WCDMA 900/2100 *Note: To query the current band, use *BAND?.* *Note: For some Mobile Network Operator SIM Cards, you may need to set the radio band before installing the SIM card.*

Table D-3: WAN/Cellular AT Commands

Command	Description
+CGDCONT	HSPA only Query or set the PDP context, APN, and other information required to establish a connection to o an HSPA network. You only need to configure this once. The parameters are saved and used each time a connection is made to the HSPA network. AT+CGDCONT? to query AT+CGDCONT = PID,PDP_TYPE,APN [,IPADDR] to set PID= PDP context identifier PDP_TYPE = numeric parameter that specifies a PDP context definition APN = Access Point Name IPADDR = IP address Examples: AT+CGDCONT=1,IP,proxy AT+CGDCONT=1,IP,internet *Note: When using the APN-related optons in ACEmanager, you generally do not need to configure +CGDCONT.*
***CLIENT_PPP_AUTH**	Query or set the Force Network Authentication mode. AT*CLIENT_PPP_AUTH? to query AT*CLIENT_PPP_AUTH=n to set • n=0—None • n=1—PAP • n=2—CHAP
+COPS	HSPA only Query or set the network operator and the connection mode. AT+COPS? to query AT+COPS=MODE[,FORMAT[,OPER]] to set MODE • MODE=0 — Automatic (default) • MODE= 1 — Manual • MODE=4 — Manual/Automatic; if manual failed, it defaults to automatic FORMAT • FORMAT=0 — Alphanumeric (“Name”) • FORMAT=2 — Numeric OPER • OPER= the operator numeric code Example, AT+COPS=1,2,302610 Manual mode, numeric format, operator code 302610 *Note: On some cellular networks, explicit use of +COPS allows you to select the roaming Mobile Network Operator to use.*

Table D-3: WAN/Cellular AT Commands

Command	Description
***EVDODATASERV**	CMDA and LTE fallback to EV-DO only. Query or set the allowable network type. AT*EVDODATASERV? to query AT*EVDODATASERV=n to set • n=0 — EV-DO Preferred — can “fall back” on CDMA/1x (only available on EV-DO devices) • n=0 — LTE Preferred — can “fall back” on CDMA/EV-DO (only available on LTE devices) • n=1 — EV-DO Only — fall back disabled (only available on 1x/EV-DO devices) • n=2 — 1x Only — EV-DO disabled (only available on 1x/EV-DO devices) • n=3—CDMA Only — LTE disabled (only available on LTE devices) • n=4—LTE Only — Fall back disabled (only available on LTE devices) *Note: If you choose one of the options where fall back is disabled and the selected network type is not available, the device will not be able to connect to the cellular network. For example, if you select LTE Only and you are in an area where there is no LTE network available, the device will not be able to connect to a cellular network until you change this setting or move to an area with LTE coverage.*
***EVDODIVERSITY**	CDMA only. For HSPA device, see *RXDIVERSITY on page 333. Query or set EV-DO Diversity, which allows two antennas to provide more consistent connection. AT*EVDODIVERSITY? to query AT*EVDODIVERSITY=n to set • n=0 — Disabled • n=1 — Enabled *Note: If you are not using a diversity antenna, *EVDODIVERSITY should be disabled.*
***EVDOROAMPREF**	CDMA and LTE fallback to EV-DO only Query or set the network roaming preference AT*EVDOROAMPREF? to query AT*EVDOROAMPREF=n to set • n=0—Automatic • n=1—Home only
***HANGUPTORESET**	HSPA only. Query or set forcing the radio module to reset when the device disconnects. AT*HANGUPTORESET? to query AT*HANGUPTORESET=n to set • n=0—Disable • n=1—Enable

Table D-3: WAN/Cellular AT Commands

Command	Description
***IPPING**	Query or set the interval between keepalive pings (in minutes) if no valid packets have been received by the IP address or FQDN specified in *IPPINGADDR. AT*IPPING? to query the keepalive PING time interval AT*IPPING=n to set the keepalive PING time interval • n=0 — Disable pinging (default) • n=15–255 minutes *Note: 15 minutes is the minimum interval for Keep Alive. If you set *IPPING for a value between 0 and 15, the idle interval for pings will be 15 minutes.*
***IPPINGADDR**	Query or set the Keepalive PING IP address or FQDN for the device to ping when Keepalive Ping Time (*IPPING) is set. AT*IPPINGADDR? to query AT*IPPINGADDR=[d.d.d.d] or [n] • d.d.d.d=IP address • n=domain name *Note: AT*IPPING must to be set to a value other than 0 to enable pinging.*
***IPPINGFORCE**	Query or set the Force Keepalive Ping setting. When this feature is enabled, the Keepalive ping is sent even if IP traffic has occurred during the configured interval. AT*IPPINGFORCE? to query AT*IPPINGFORCE=n to set • n=0—Disable • n=1—Enable *Note: To enable this command, *IPPING must be enabled and *IPPINGADDR configured.*
***NETALLOWZEROIP**	Query or set allowing the device to get an IP address from the cellular network that has the last octet as 0 (zero). AT*NETALLOWZEROIP? to query AT*NETALLOWZEROIP=n to set • n=0 — Do not allow • n=1 — Allow Allows the device to use a WAN IP address that ends in zero (e.g. 192.168.1.0).
***NETAPN**	HSPA and LTE fallback to HSPA only Query or set the user entered APN. AT*NETAPN? to query AT*NETAPN=APN to set (up to 80 characters) *Note: When you set this command, the APN type is automatically set to User Entry so that the APN you enter with this AT command is used on reboot.*

Table D-3: WAN/Cellular AT Commands

Command	Description
***NETPW**	Set the cellular network account password, if required. AT*NETPW=PW to set (up to 30 characters) *Note: AT*NETPW? returns a dotted display for privacy.*
***NETUID**	Query or set the cellular network account user ID, if required. AT*NETUID? to query AT*NETUID=USER ID (up to 64 bytes)
***NETWDOG**	Query or set the interval (in minutes) that the network connection watchdog waits for a network connection. If no connection is established within this interval, the device resets. AT*NETWDOG? to query AT*NETWDOG=n to set • n=0—Disable • n=1–255 (minutes) default is 120
PING	Sends 5 PING to a single address. Returns OK if there is a response: ERROR if there is no response. ATPING[ip address or FQDN] *Note: Do not use an equal sign (=) when issuing the command.* Example: ATPINGsierrawireless.com
$QCMIP	CDMA and LTE fallback to EV-DO only Query or set use of Mobile IP (MIP) preferences. $QCMIP? to query $QCMIP=n to set • n=0—Disabled, Simple IP (SIP) only • n=1—Mobile IP preferred • n=2—Mobile IP only

Table D-3: WAN/Cellular AT Commands

Command	Description

***RADIO_CONNECT**	HSPA only
	Query or set the wireless connection setting.
	AT*RADIO_CONNECT? to query
	AT*RADIO_CONNECT=n to set
	• n=0—Disables data traffic. The only way to change this mode is to issue a radio_connect=1 or radio_connect=2 AT command.
	• n=1—Enables Always on connection.
	• n=2—Disables Always on connection. The device listens for outgoing traffic and establishes a mobile network data connection for a specified time:
	  • When there is outgoing traffic
	  or
	  • When it receives a Wakeup SMS, provided Wakeup SMS is configured.
	  (Use *TRAFWUPTOUT on page 334 to set the timeout period.)
	Note: This command is not persistent over device resets.
	Note: You can only send this command locally over a serial, serial USB, or local telnet/SSH connection.

***RADIO_CONNECT_ STARTUP**	HSPA only This command is the same as *RADIO_CONNECT, except • The change does not take effect until the next reboot. • The setting is persistent over subsequent reboots.
***RXDIVERSITY**	HSPA only. For CDMA devices, see *EVDODIVERSITY on page 330. Query or set the RX Diversity setting. Rx Diversity allows you to use two antennas for a more consistent connection. If you are not using a diversity antenna, Rx Diversity should be disabled. AT*RXDIVERSITY? to query AT*RXDIVERSITY=n to set • n=0—Disable • n=1—Enable *Note: This AT Command is not available for all AirLink devices.*
***SIMPIN**	HSPA and LTE fallback to HSPA only Query or enter the SIM pin. AT*SIMPIN? to query AT*SIMPIN=n to enter the SIM pin

Table D-3: WAN/Cellular AT Commands

Command	Description
***SIMPINENABLE**	HSPA and LTE fallback to HSPA only Query or set the SIM pin. AT*SIMPINENABLE? to query AT*SIMPINENABLE=n to set • n=0—Don't change • n=1—Enable (SIM pin required on startup) • n=2—Disable
***TRAFWUPTOUT**	HSPA only Query or set the timeout period after which, if there is no outgoing WAN traffic the connection is terminated. The timeout period only takes effect if *RADIO_CONNECT or *RADIO_CONNECT_STARTUP is set to 1, or Always on connection is disabled in ACEmanager. (See Always on connection on page 110.) AT*TRAFWUPTOUT? to query AT*TRAFWUPTOUT=n to set • n=2–65535 minutes (default is 2) *Note: This timer is reset to zero each time a WAN packet goes out.*

LAN/WiFi

LAN

Note: A reboot is required before these commands take effect.

Table D-4: LAN AT Commands

Command	Description
***DHCPHOSTEND**	Query or set the ending IP address for the Ethernet DHCP pool AT*DHCPHOSTEND? to query AT*DHCPHOSTEND=d.d.d.d to set • d.d.d.d=last IP address in Ethernet DHCP pool
***DHCPNETMASK**	Query or set the Ethernet DHCP subnet mask AT*DHCPNETMASK? to query AT*DHCPNETMASK=d.d.d.d to set • d.d.d.d=Ethernet DHCP subnet mask
***DHCPSERVER**	Query or set the Ethernet DHCP server. AT*DHCPSERVER? to query AT*DHCPSERVER=n to enable or disable the DHCP server mode • n=0—Disable • n=1—Enable

Table D-4: LAN AT Commands (Continued)

Command	Description
***DNS1?** ***DNS2?**	Query the primary DNS (*DNS1) and secondary (*DNS2) IP addresses. AT*DNS1? to query DNS1 AT*DNS2? to query DNS2
***DNSUSER**	Query or set the first alternate server for DNS override. (Applies only to primary DNS.) AT*DNSUSER? to query AT*DNSUSER=d.d.d.d • d.d.d.d=IP address of domain server
***HOSTAUTH**	Query or set the Host Authentication mode for PPPoE only. (It does not set host authentication for PPP/DUN.) AT*HOSTAUTH? to query AT*HOSTAUTH=n to set • n=0—None/Disables authentication for PPPoE (Default). • n=1— Authentication through PAP • n=2—Authentication through PAP & CHAP
***HOSTPEERIP**	Query or set the IP address of the device's Ethernet port. By default this is 192.168.13.31. *Note: Any connected LAN host can access this IP addresses, whether using a private or public IP address. This IP address must be in the same subnet as the Ethernet DHCP pool.* AT*HOSTPEERIP? to query AT*HOSTPEERIP=d.d.d.d to set • d.d.d.d=local or peer IP address of the device
***HOSTPRIVIP**	Query or set the starting IP for the Ethernet DHCP pool. AT*HOSTPRIVIP? to query AT*HOSTPRIVIP=d.d.d.d to set • d.d.d.d=IP Address
***HOSTPRIVMODE**	Query or set the host communication mode used for tethered IP connections. AT*HOSTPRIVMODE? to query AT*HOSTPRIMODE=n to set which user interface uses the Public IP address • n=0—Ethernet Uses Public IP • n=1—All Hosts Use Private IPs • n=2—USB Uses Public IP • n=3—DUN Uses Public IP • n=4—First Host gets Public IP
***HOSTPW**	Query or set the host password for PPPoE only. (It does not set the password for PPP/DUN.) AT*HOSTPW? to query AT*HOSTPW=PASSWORD to set *Note: PASSWORD cannot be "password".*

Table D-4: LAN AT Commands (Continued)

Command	Description
***HOSTUID**	Query or set the Host user ID for PPPoE only. (It does not set the user ID for PPP/DUN.) AT*HOSTUID? to query AT*HOSTUID=USER ID to set (up to 64 bytes) *Note: USER ID cannot be "user".*
***USBDEVICE**	Query or set the USB Device Mode. This parameter alters the default startup data mode. AT*USBDEVICE? to query AT*USBDEVICE=n to set • n=0— USB Serial • n=1— USBNET • n=2— Disabled

Wi-Fi

Wi-Fi AT Commands are only applicable if the AirLink device has an installed Wi-Fi X-Card and is in Access Point Mode.

Note: You need to configure Client Mode in ACEmanager. There is no AT Command for Wi-Fi Client mode. See WiFi Mode on page 72.

Note: A reboot is required before these commands take effect.

Table D-5: Wi-Fi AT Commands

Command	Description
***APBRIDGED**	Query or set the Bridge Wi-Fi Access Point to Ethernet feature. AT*APBRIDGED? to query AT*APBRIDGED=n to set • n=0 —Disable • n=1 —Enable
***APCHANNEL**	Query or set the Wi-Fi Access Point channel to use. AT*APCHANNEL? to query AT*APCHANNEL=n to set • n = 1 – 11 (available channels)
***APEN**	Query or set the Wi-Fi Access Point mode. AT*APEN? to query AT*APEN=n to set • n=2 —b/g Enabled • n=3 —b/g/n Enabled

Table D-5: Wi-Fi AT Commands (Continued)

Command	Description
***APENDIP**	Query or set the ending IP address for the Wi-Fi Access Point DHCP pool. AT*APENDIP? to query AT*APENDIP=d.d.d.d to set • d.d.d.d= IP Address
***APHOSTIP**	Query or set the Host Wi-Fi Access Point device IP address. AT*APHOSTIP? to query AT*APHOSTIP=d.d.d.d to set • d.d.d.d= IP Address
***APMAXCLIENT**	Query or set the maximum number of Wi-Fi Access Point clients. AT*APMAXCLIENT? to query AT*APMAXCLIENT=n to set • n=0–8
***APNETMASK**	Query or set the Wi-Fi DHCP subnet mask. AT*APNETMASK? to query AT*APNETMASK=d.d.d.d to set • d.d.d.d = IP Address
***APSECURITYTYPE?**	Query the Wi-Fi Access Point Security Encryption type. AT*APSECURITYTYPE? • n=0—Open (WEP encryption) • n=3—WPA Personal • n=5—WPA2 Personal *Note: WEP is not a recommended Wi-Fi Security protocol because of its vulnerabilities and because only alphanumeric characters can be used for the passphrase. Use WPA/WPA2 instead.*
***APSSIDBCAST**	Query or set the broadcast Wi-Fi Access Point SSID. AT*APSSIDBCAST? to query AT*APSSIDBCAST=n to set • n=0 —Disable • n=1 —Enable
***APSSIDVAL**	Query or set the Access Point SSID/Network name. AT*APSSIDVAL? to query AT*APSSIDVAL=n to set • n = ASCII SSID STRING
***APSTARTIP**	Query or set the Query or set the Access Point DHCP start of IP address pool. AT*APSTARTIP? to query AT*APSTARTIP=d.d.d.d to set • d.d.d.d= IP Address

Table D-5: Wi-Fi AT Commands (Continued)

Command	Description
***APTXPWR**	Query or set the Wi-Fi Access Point Transmit Power mode. AT*APTXPWR? to query AT*APTXPWR=n to set • n=0—Low • n=1—Normal
***APWEPENCTYPE?**	Query the Wi-Fi Access Point WEP encryption type. AT*APWEPENCTYPE? • n=0—Disabled (Open) • n=1—WEP *Note: WEP is not a recommended Wi-Fi Security protocol because of its vulnerabilities and because only alphanumeric characters can be used for the passphrase. Use WPA/WPA2 instead.*
***APWEPKEY?**	Query the Wi-Fi Access Point WEB key generated at boot from the WEP passphrase. AT*APWEPKEY?
***APWEPKEYLEN?**	Query the length of the Wi-Fi Access Point WEP key. AT*APWEPKEYLEN? • n=0—64-bit • n=1—128-bit • n=2—Custom
***APWPACRYPT?**	Query the Wi-Fi Access Point WPA/WPA2 encryption type. AT*APWEPKEY? • n=0—TKIP • n=1—AES *Note: If you are using WPA2, only AES is allowed.*
WCC?	Query the Wi-Fi country code.
***WIFIMAC?**	Query the MAC address of the Wi-Fi Access Point. *Note: Wi-Fi Client uses a different MAC address.*
***WIFIMODE**	Query or set the WI-Fi Mode. AT*WIFIMODE? to query AT*WIFIMODE=n to set • n=0—Disabled • n=1—AP (Access Point) • n=2—Client • n=3—AP and Client For more information, see Wi-Fi on page 85.

VPN

Table D-6: VPN Commands

Command	Description
***IPSEC1_AUTH** ***IPSEC2_AUTH** ***IPSEC3_AUTH** ***IPSEC4_AUTH** ***IPSEC5_AUTH**	Query or set the authentication type for # VPN. AT*IPSEC[VPN number]_AUTH? to query AT*IPSEC[VPN number]_AUTH=n to set • n=0 — None • n=1 — MD5 • n=2 — SHA1 (default) • n=3 — SHA 256 *Note: MD5 is an algorithm that produces a 128-bit digest for authentication. SHA is a more secure algorithm that produces both 160-bit (SHA1) and 256-bit (SHA256) digests.*
***IPSEC1_DH** ***IPSEC2_DH** ***IPSEC3_DH** ***IPSEC4_DH** ***IPSEC5_DH**	Query or set how the AirLink Device VPN creates an SA with the VPN server. The DH (Diffie-Hellman) key exchange protocol establishes pre-shared keys during the phase 1 authentication. The AirLink Device supports three prime key lengths, including Group 1 (768 bits), Group 2 (1,024 bits), and Group 5 (1,536 bits). AT*IPSEC[VPN number]_DH? to query AT*IPSEC[VPN number]_DH=n to set • n=0 — None • n=1 — DH1 • n=2 — DH2 (default) • n=5 — DH5
***IPSEC1_ENCRYPT** ***IPSEC2_ENCRYPT** ***IPSEC3_ENCRYPT** ***IPSEC4_ENCRYPT** ***IPSEC5_ENCRYPT**	Query or set the type/length of encryption key used to encrypt/decrypt ESP (Encapsulating Security Payload) packets for # VPN. AT*IPSEC[VPN number]_ENCRYPT? to query AT*IPSEC[VPN number]_ENCRYPT=n to set • n=0 — None • n=1 — DES • n=2 — 3DES • n=3 — AES-128 (default) • n=7 — AES-256 *Note: 3DES supports 168-bit encryption. AES (Advanced Encryption Standard) supports both 128-bit and 256-bit encryption.*
***IPSEC1_GATEWAY** ***IPSEC2_GATEWAY** ***IPSEC3_GATEWAY** ***IPSEC4_GATEWAY** ***IPSEC5_GATEWAY**	Query or set the IP address of the server that # VPN client connects to. AT*IPSEC[VPN number]_GATEWAY? to query AT*IPSEC[VPN number]_GATEWAY=[IP address] to set

Table D-6: VPN Commands (Continued)

Command	Description
***IPSEC1_IKE_AUTH** ***IPSEC2_IKE_AUTH** ***IPSEC3_IKE_AUTH** ***IPSEC4_IKE_AUTH** ***IPSEC5_IKE_AUTH**	Query or set the IKE authentication type for # VPN. AT*IPSEC[VPN number]_IKE_AUTH? to query AT*IPSEC[VPN number]_IKE_AUTH=n to set • n=1 — MD5 • n=2 — SHA1 • n=3 — SHA 256 *Note: MD5 is an algorithm that produces a 128-bit digest for authentication. SHA is a more secure algorithm that produces both 160-bit (SHA1) and 256-bit (SHA256) digests.*
***IPSEC1_IKE_DH** ***IPSEC2_IKE_DH** ***IPSEC3_IKE_DH** ***IPSEC4_IKE_DH** ***IPSEC5_IKE_DH**	Query or set how the AirLink Device VPN creates an SA with the VPN server. The DH (Diffie-Hellman) key exchange protocol establishes pre-shared keys during the phase 1 authentication. The AirLink Device supports three prime key lengths, including Group 1 (768 bits), Group 2 (1,024 bits), and Group 5 (1,536 bits). AT*IPSEC[VPN number]_IKE_DH? to query AT*IPSEC[VPN number]_IKE_DH=n to set • n=1 — DH1 • n=2 — DH2 (default) • n=5 — DH5
***IPSEC1_IKE_ENCRYPT** ***IPSEC2_IKE_ENCRYPT** ***IPSEC3_IKE_ENCRYPT** ***IPSEC4_IKE_ENCRYPT** ***IPSEC5_IKE_ENCRYPT**	Query or set the type/length of IKE encryption key used to encrypt/decrypt ESP (Encapsulating Security Payload) packets for # VPN. AT*IPSEC[VPN number]_IKE_ENCRYPT? to query AT*IPSEC[VPN number]_IKE_ENCRYPT=n to set • n=1 — DES • n=5 — 3DES • n=7 — AES-128 (default) • n=9 — AES-256 *Note: 3DES supports 168-bit encryption. AES (Advanced Encryption Standard) supports both 128-bit and 256-bit encryption.*
***IPSEC1_IKE_LIFETIME** ***IPSEC2_IKE_LIFETIME** ***IPSEC3_IKE_LIFETIME** ***IPSEC4_IKE_LIFETIME** ***IPSEC5_IKE_LIFETIME**	Query or set how long the # VPN tunnel is active (in seconds). AT*IPSEC[VPN number]_IKE_LIFETIME? to query AT*IPSEC[VPN number]_IKE_LIFETIME=n to set • n= 180–86400 • Default is 7200.
***IPSEC1_LIFETIME** ***IPSEC2_LIFETIME** ***IPSEC3_LIFETIME** ***IPSEC4_LIFETIME** ***IPSEC5_LIFETIME**	Query or set how long the # VPN tunnel is active (in seconds). AT*IPSEC[VPN number]_LIFETIME? to query AT*IPSEC[VPN number]_LIFETIME=n to set • n= 180–86400 • Default is 7200.

Table D-6: VPN Commands (Continued)

Command	Description
***IPSEC1_LOCAL_ADDR** ***IPSEC2_LOCAL_ADDR** ***IPSEC3_LOCAL_ADDR** ***IPSEC4_LOCAL_ADDR** ***IPSEC5_LOCAL_ADDR**	Query or set the device subnet address for # VPN. AT*IPSEC[VPN number]_LOCAL_ADDR? returns the device subnet address AT*IPSEC[VPN number]_LOCAL_ADDR=[subnet address] to set
***IPSEC1_LOCAL_ADDR_NETMASK** ***IPSEC2_LOCAL_ADDR_NETMASK** ***IPSEC3_LOCAL_ADDR_NETMASK** ***IPSEC4_LOCAL_ADDR_NETMASK** ***IPSEC5_LOCAL_ADDR_NETMASK**	Query or set the device subnet mask information (24-bit netmask) AT*IPSEC[VPN number]_LOCAL_ADDR_NETMASK? to query AT*IPSEC[VPN number]_LOCAL_ADDR=[subnet mask] to set Default is 255.255.255.0
***IPSEC1_LOCAL_ADDR_TYPE** ***IPSEC2_LOCAL_ADDR_TYPE** ***IPSEC3_LOCAL_ADDR_TYPE** ***IPSEC4_LOCAL_ADDR_TYPE** ***IPSEC5_LOCAL_ADDR_TYPE**	Query or set the network address type for # VPN. AT*IPSEC[VPN number]_LOCAL_ADDR_TYPE? to query AT*IPSEC[VPN number]_LOCAL_ADDR_TYPE=n to set • n=1 — Use the Host Subnet • n=5 — Single Address • n=17 — Subnet Address (default)
***IPSEC1_LOCAL_ID** ***IPSEC2_LOCAL_ID** ***IPSEC3_LOCAL_ID** ***IPSEC4_LOCAL_ID** ***IPSEC5_LOCAL_ID**	Query or set the local (My Identity) ID for the # VPN. • If IP is selected as the local (My Identity) type, AT*IPSEC[VPN number]_LOCAL _ID? returns the WAN IP address assigned by the Mobile Network Operator • If FQDN or User FQDN is selected as the local (My Identity) type, AT*IPSEC[VPN number]_LOCAL_ID? returns the FQDN (for example me@mycompany.com) To set the local ID: AT*IPSEC[VPN number]_LOCAL _ID=[IP address] or [FQDN], depending on the setting for Local ID (My Identity) type.
***IPSEC1_LOCAL_ID_TYPE** ***IPSEC2_LOCAL_ID_TYPE** ***IPSEC3_LOCAL_ID_TYPE** ***IPSEC4_LOCAL_ID_TYPE** ***IPSEC5_LOCAL_ID_TYPE**	Query or set the local (My Identity) ID type for the # VPN. AT*IPSEC[VPN number]_LOCAL_ID_TYPE? to query AT*IPSEC[VPN number]_LOCAL_ID_TYPE=n to set • n=1 — IP • n=2 — FQDN • n=3 — User FQDN *Note:* • *IP (default) allows you to use an IP address* • *FQDN allows you to use a fully qualified domain name (FQDN) e. g., modemname.domainname.com* • *User FQDN allows you to use a user FQDN whose values should include a username (e.g. user@domain.com)*

Table D-6: VPN Commands (Continued)

Command	Description
***IPSEC1_NEG_MODE** ***IPSEC2_NEG_MODE** ***IPSEC3_NEG_MODE** ***IPSEC4_NEG_MODE** ***IPSEC5_NEG_MODE**	Query or set the negotiation mode for # VPN. AT*IPSEC[VPN number]_NEG_MODE? returns AT*IPSEC[VPN number]_NEG_MODE=n to set • n=1 — Main • n=2 — Aggressive *Note: Aggressive mode offers increased performance at the expense of security.*
***IPSEC1_PFS** ***IPSEC2_PFS** ***IPSEC3_PFS** ***IPSEC4_PFS** ***IPSEC5_PFS**	Query or set the Perfect Forward Secrecy (PFS) setting for # VPN. PFS provides additional security through a DH shared secret value. When this feature is enabled, one key cannot be derived from another. This ensures previous and subsequent encryption keys are secure even if one key is compromised. AT*IPSEC[VPN number]_PFS? to query PFS AT*IPSEC[VPN number]_PFS=n to set PFS • n=0 — Yes (default) • n=1 — No
***IPSEC1_REMOTE_ADDR** ***IPSEC2_REMOTE_ADDR** ***IPSEC3_REMOTE_ADDR** ***IPSEC4_REMOTE_ADDR** ***IPSEC5_REMOTE_ADDR**	Query or set the IP address of the device behind the gateway for # VPN. AT*IPSEC[VPN number]_REMOTE_ADDR? to query AT*IPSEC[VPN number]_REMOTE_ADDR=[IP address] to set
***IPSEC1_REMOTE_ADDR_TYPE** ***IPSEC2_REMOTE_ADDR_TYPE** ***IPSEC3_REMOTE_ADDR_TYPE** ***IPSEC4_REMOTE_ADDR_TYPE** ***IPSEC5_REMOTE_ADDR_TYPE**	Query or set network information of the IPsec server behind the IPsec gateway for # VPN. AT*IPSEC[VPN number]_REMOTE_ADDR_TYPE? to query AT*IPSEC[VPN number]_REMOTE_ADDR_TYPE=n to set • n=5 — Single Address • n=17 — Subnet Address (default)
***IPSEC1_REMOTE_ADDR_NETMASK** ***IPSEC2_REMOTE_ADDR_NETMASK** ***IPSEC3_REMOTE_ADDR_NETMASK** ***IPSEC4_REMOTE_ADDR_NETMASK** ***IPSEC5_REMOTE_ADDR_NETMASK**	Query or set the remote subnet mask information (24-bit netmask). AT*IPSEC[VPN number]_REMOTE_ADDR_NETMASK? to query AT*IPSEC[VPN number]_REMOTE_ADDR=[subnet mask] to set Default is 255.255.255.0
***IPSEC1_REMOTE_ID** ***IPSEC2_REMOTE_ID** ***IPSEC3_REMOTE_ID** ***IPSEC4_REMOTE_ID** ***IPSEC5_REMOTE_ID**	Query or set the remote (Peer Identity) ID for the # VPN. • If IP is selected as the remote (Peer Identity) type, AT*IPSEC[VPN number]_REMOTE_ID? returns the WAN IP address assigned by the Mobile Network Operator • If FQDN or User FQDN is selected as the remote (Peer Identity) type, AT*IPSEC[VPN number]_REMOTE_ID? returns the FQDN (for example me@mycompany.com) To set the remote ID: AT*IPSEC[VPN number]_REMOTE _ID=[IP address] or [FQDN], depending on the setting for remote ID (Peer Identity) type.

Table D-6: VPN Commands (Continued)

Command	Description
***IPSEC1_REMOTE_ID_TYPE** ***IPSEC2_REMOTE_ID_TYPE** ***IPSEC3_REMOTE_ID_TYPE** ***IPSEC4_REMOTE_ID_TYPE** ***IPSEC5_REMOTE_ID_TYPE**	Query or set the remote (Peer Identity) ID type for the # VPN. AT*IPSEC[VPN number]_REMOTE_ID_TYPE? to query AT*IPSEC[VPN number]_REMOTE_ID_TYPE=n to set • n=1 — IP • n=2 — FQDN • n=3 — User FQDN *Note:* • *FQDN allows you to use a fully qualified domain name (FQDN) e. g., modemname.domainname.com* • *User FQDN allows you to use a user FQDN whose values should include a username (e.g. user@domain.com)*
***IPSEC1_SHARED_KEY1** ***IPSEC2_SHARED_KEY1** ***IPSEC3_SHARED_KEY1** ***IPSEC4_SHARED_KEY1** ***IPSEC5_SHARED_KEY1**	Query the pre-shared Key (PSK) used to initiate the # VPN tunnel. AT*IPSEC[n]_SHARED_KEY1? [n]=server number
***IPSEC1_STATUS?** ***IPSEC2_STATUS?** ***IPSEC3_STATUS?** ***IPSEC4_STATUS?** ***IPSEC5_STATUS?**	Query the VPN # connection status. AT*IPSEC[VPN number]_STATUS? to query • Disabled • Not Connected • Connected *Note: Use this when troubleshooting a VPN # connection.*
***IPSEC1_TUNNEL_TYPE** ***IPSEC2_TUNNEL_TYPE** ***IPSEC3_TUNNEL_TYPE** ***IPSEC4_TUNNEL_TYPE** ***IPSEC5_TUNNEL_TYPE**	Query or set the VPN # tunnel type. AT*IPSEC[VPN number]_TUNNEL_TYPE? to query AT*IPSEC[VPN number]_TUNNEL_TYPE=n to set • n=0 — Disable the tunnel (default) • n=1 — IPsec Tunnel • n=2 — GRE Tunnel • n=3 — SSL Tunnel *Note: For a successful configuration, all settings for the VPN tunnel must be identical between the AirLink Device VPN and the enterprise VPN server.*

Security

Table D-7: Security AT Commands

Command	Description
F0 (F1, F2, ... F9)	Query or set the Inbound Trusted IP List. ATF? to query the list ATF[n]=d.d.d.d to set • n=0–9 Trusted IP list index number • d.d.d.d = IP Address Using 255 in the IP address will allow any number Example: 166.129.2.255 allows access by all IPs in the range 166.129.2.0–166.129.2.255. Example: atf? 0=192.32.32.21 1=192.32.32.22 2=192.32.32.23 3=0.0.0.0 4=0.0.0.0 5=0.0.0.0 6=0.0.0.0 7=0.0.0.0 8=0.0.0.0 9=0.0.0.0 OK If the index number does not have an IP address associated with it, the query returns 0.0.0.0 for that index number. *Note: You can only query or configure the first nine Inbound Trusted IP addresses with this AT Command. You cannot query or configure Trusted range entries with this AT Command.*
FM	Query or set the Inbound Trusted IP mode (Friends List) — Only allow specified IPs to access the device. ATFM? to query the setting ATFM=n to set • n=0 — Disable Trusted IP mode • n=1 — Enable Trusted IP mode — Only packets from IP addresses in the Trusted IP list are allowed. Packets from other IP addresses are ignored.

Services

Table D-8: Services AT Commands

Command	Description
AirVantage Management System	
***AVMS_ENABLE**	Query or set the AVMS activation status. AT*AVMS_ENABLE? to query AT*AVMS_ENABLE=n to set • n=0—Disable device initiated AVMS management • n=1—Enable device initiated AVMS management
***AVMS_INTERVAL**	Query or set the AVMS communication (heartbeat) interval in seconds. AT*AVMS_INTERVAL? to query AT*AVMS_INTERVAL= n to set • n= INTERVAL (in seconds)
***AVMS_NAME**	Assigns or queries the name to the AirLink device as it appears in AVMS. AT*AVMS_NAME? to query AT*AVMS_NAME= n to set • n= AVMS NAME
***AVMS_SERVER**	Query or set the AVMS server IP address or FQDN. AT*AVMS_SERVER? to query AT*AVMS_SERVER=n to set • n=IP Address or FQDN of AVMS server
***AVMS_STATUS?**	Query the AVMS connection status
Low Power	
***ENGHRS**	Query or set the number of hours the engine has been running. AT*ENGHRS? to query AT*ENGHRS=n to set • n= HOURS Maximum value is 65535.
***POWERMODE?**	Query the current power state/mode. AT*POWERMODE? returns: • Initial—The device is in the initial 5 minutes since power up, so power down event will be ignored • On—Regular power on, a power down is not pending • Low Cancellable—Power down is pending but still Cancellable if the power down trigger goes away • Low Pending 1 and Low Pending 3—Power down is pending, any device tasks are gracefully preparing for the power down • Low Final—Power down is imminent • Low—Power is down

Table D-8: Services AT Commands

Command	Description
PTMR	Query or set the Low Power Mode Delay (in minutes) This is the delay between the time the power down trigger occurs and when the device enters the low power mode. ATPTMR? to query ATPTMR=n to set • n=0–255 (minutes) *Note: There is always a minimum of 1 minute between power down event and actual shutdown (to give the device time to prepare); entering zero will not power down the device immediately.*
VLTG	Query or set the voltage level (threshold for low power mode). When the power drops below this level Low Power Mode is triggered. ATVLTG? to query ATVLTG=n to set • n= 0—Ignore voltage for power control • n= 80–360—threshhold in .1 volt units Example: ATVLTG=130 would place the device in a low power use, standby state if the voltage goes below 13.0V.
Dynamic DNS	
***DOMAIN**	Query or set the domain name used for the IP Manager Dynamic DNS configuration. AT*DOMAIN? to query AT*DOMAIN=DOMAIN to set (up to 20 characters) Example: AT*DOMAIN=eairlink.com **Tip:** *Only letters, numbers, hyphens, and periods can be used in a domain name.* *Note: This AT command is only usable if the Dynamic DNS Service type is set to IP Manager.*
***DYNDNS**	Query or set the Dynamic DNS Service type to use. AT*DYNDNS? to query AT*DNYDNS=n to set • n=0—Disable (default) • n=2—dyndns.org • n=5—noip.org • n=6—ods.org • n=8—regfish.com • n=9—tzo.org • n=10—IP Manager *Note: Only IP Manager can be fully configured using AT Commands.*

Table D-8: Services AT Commands

Command	Description
***IPMANAGER1** ***IPMANAGER2**	*Note: This AT command is only usable if the Dynamic DNS Service type is set to IP Manager.* Query or set a FQDN or IP address of the IP server to send IP change notifications to. You can configure two independent IP Manager servers. AT*IPMANAGER[n]? to query AT*IPMANAGER[n]=SERVER to set. • n=1—First IP Manager server • n=2—Second IP Manager server • SERVER = Server FQDN or IP address *Note:* You can disable updates to a server by setting blank entry (e.g., “AT*IPMANAGER1=”).
***IPMGRKEY1** ***IPMGRKEY2**	*Note: This AT command is only usable if the Dynamic DNS Service type is set to IP Manager.* Query or set the 128-bit password/key used to authenticate the IP update notifications. If the key's value is all zeros, a default key is used. If all the bytes in the key are set to FF, then no key is used (i.e., the IP change notifications will not be authenticated). AT*IPMGRKEY[n]? to query AT*IPMANAGER[n]=KEY to set • n=1—First IP Manager server • n=2—Second IP Manager server • KEY=128-bit key in hexadecimal [32 hex characters]
***IPMGRUPDATE1** ***IPMGRUPDATE2**	*Note: This AT command is only usable if the Dynamic DNS Service type is set to IP Manager.* Query or set the interval (in minutes) to send an IP update notification to the corresponding server. This occurs even if the IP address of the device does not change. If the value is set to 0, then periodic updates are not issued (i.e., IP change notifications is only be sent when the IP actually changes). AT*IPMGRUPDATE[n] to query AT*IPMGRUPDATE[n]=INTERVAL to set • n=0—Disables the update interval (updates only on changes) • n=1—First IP Manager server • n=2—Second IP Manager server • INTERVAL=1–255—interval (in minutes) to send an update

Table D-8: Services AT Commands

Command	Description
***MODEMNAME**	*Note: This AT command is only usable if AT*DYNDNS is set to 10 (IP Manager).* Query or set the device name used by IP Manager. (This name is displayed on the Status > Home page.) AT*MODEMNAME? to query AT*MODEMNAME=NAME to set (up to 20 characters long) • NAME= device name (for example, mydevice) The value in *DOMAIN provides the domain zone to add to this name. Example: If *MODEMNAME=mydevice and *DOMAIN=eairlink.com, the device's fully qualified domain name is mydevice.eairlink.com. **Tip:** *Each device using IP Manager needs a unique name. I.e., two devices cannot both be called "mydevice". One could be named "mydevice1" while the other could be named "mydevice2".*
SMS	

***SMSM2M**
***SMSM2M_8**
***SMSM2M_u**
	• AT*SMSM2M sends an SMS in ASCII text (requires quotation marks; maximum 140 characters)
	• AT*SMSM2M_8 sends an 8-bit SMS (requires quotation marks; maximum 140 characters)
	• AT*SMSM2M_U sends a unicode SMS (requires quotation marks; maximum 140 characters)
	Format:
	AT*SMSM2M="[phone] [ascii message]"
	AT*SMSM2M_8="[phone] [hex message]"
	AT*SMSM2M_U="[phone] [hex message]"
	• The phone number can only consist of numbers (NO spaces or other characters). The phone number should be as it appears in the Last Incoming Phone Number field.
	  • Example 1 (US): 14085551212 (including leading 1 and area code)
	  • Example 2 (US): 4085551212 (ignore leading 1, include area code)
	  • Example 3 (UK): 447786111717 (remove leading 0 and add country code)
	Command Examples:
	AT*SMSM2M="18005551212 THIS IS A TEST" sends in ASCII.
	AT*SMSM2M_8="17604053757 5448495320495320412054455354" sends the message "THIS IS A TEST" as 8-bit data.
	AT*SMSM2M_U="17604053757 000102030405060708090a0b0c0d0e0f808182838485868788898A8b8c8d8e8f" sends the bytes:
	00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
	80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f
	
	Note: Not all cellular Mobile Network Operators support 8-bit or unicode SMS messages.

Table D-8: Services AT Commands

Command	Description
***SMS_PASSWORD**	Query or set the SMS password. AT*SMS_PASSWORD? to query AT*SMS_PASSWORD = n n= SMS password If no password has ever been configured, a default password is created from the last four characters of the SIM ID (for all SIM-based devices) or the ESN (for devices without a SIM, such those using EV-DO). *Note: The configured password remains in place, even when the device is reset to factory default settings.*
***SMSWUPTOUT**	HSPA only Query or set the connection timeout for the SMS Wakeup feature. When this feature is enabled, an IP connection is initiated on receipt of a specific type of SMS. The IP connection closes after the timeout period specified in this AT command. Outgoing traffic sent after the timer is set does not reset the timer. AT*SMSWUPTOUT? to query AT*SMSWUPTOUT=n to set • n=2–65535 minutes (default is 2) See also *RADIO_CONNECT on page 333.
Telnet/SSH	
***TELNETTIMEOUT**	Query or set the Telnet/SSH idle time out. By default, this value is set to close the telnet/SSH connection if no data is received for 2 minutes. AT*TELNETTIMEOUT? to query AT*TELNETTIMEOUT=n to set • n=1—255 minutes (Default is 2.)
***TSSH**	Query or set the remote login server mode. AT*TSSH? to query AT*TSSH=n to set • n=0—Telnet (default) • n=1—SSH
***TPORT**	Query or set the Telnet/SSH port. AT*PORT? to query AT*PORT=n to set • n=1–65535 (Default is 2332.) Many networks have the ports below 1024 blocked. It is recommended to use a higher numbered port.
Management (SNMP)	
SNMP General Configuration	

Table D-8: Services AT Commands

Command	Description
***SNMP**	Query or set the SNMP option. AT*SNMP? to query AT*SNMP=n to set • n=0—Disable • n=1—Enable
***SNMPCONTACT**	Add string contact information in SNMPv2 and SNMPv3. AT*SNMPCONTACT=string • string= email address (Example: admin@sierrawireless.com)
***SNMPLOCATION**	Add string location information in SNMPv2 and SNMPv3. AT*SNMPLOCATION=string • string= location information (Example: Building 19–67B)
***SNMPNAME**	Add string name in SNMPv2 and SNMPv3. AT*SNMPNAME=STRING • STRING=name (Example: John Doe)
***SNMPPORT**	Query or set the port number in SNMPv2 and SNMPv3. AT*SNMPPORT? to query AT*SNMPPORT=n to set • n=1–65535 (Default is 161.)
***SNMPVERSION**	Query or set the SNMP version. AT*SNMPVERSION? to query AT*SNMPVERSION=n to set • n=2—version 2 • n=3—version 3
SNMP Read Only Configuration	
***SNMPPROCOMMUNITY**	Read-only community string in SNMPv2 and SNMPv3 (SNMP equivalent of a password; for example: public)
***SNMPROUSER**	Query or set a read only SNMP username string in SNMPv3.
***SNMPROUSERAUTHTYPE**	Query or set the read only authentication type in SNMPv3. AT*SNMPROUSERAUTHTYPE? to query AT*SNMPROUSERAUTHTYPE=n • n=0—MD5 • n=1—SHA
***SNMPROUSERSECLVL**	Query or set the read only security level in SNMPv3. AT*SNMPROUSERSECLVL? to query AT*SNMPROUSERSECLVL=n to set • n=0—none • n=1—authentication only • n=2—authentication + privacy
SNMP Read/Write Configuration	

Table D-8: Services AT Commands

Command	Description
***SNMPRWCOMMUNITY**	Read/write community string in SNMPv2 and SNMPv3. (SNMP equivalent of a password; for example: private)
***SNMPRWUSER**	Query or set a read/write SNMP username string in SNMPv2 and SNMPv3.
***SNMPRWUSERAUTHTYPE**	Query or set the read/write authentication type in SNMPv3. AT*SNMPRWUSERAUTHTYPE? to query AT*SNMPRWUSERAUTHTYPE=n to set • n=0—MD5 • n=1—SHA
***SNMPRWUSERSECLVL**	Query or set the read/write security level in SNMPv3. AT*SNMPRWUSERSECLVL? to query AT*SNMPRWUSERSECLVL=n to set • n=0—none • n=1—authentication only • n=2—authentication + privacy
***SNMPRWUSERPRIVTYPE**	Query or set the read/write privacy type in SNMPv3. AT*SNMPRWUSERPRIVTYPE? to query AT*SNMPRWUSERPRIVTYPE=n to set • n=0—DES • n=1—AES
SNMP TRAP Configuration	
***SNMPENGINEID**	Specify an identification name string for a SNMP engine in SNMPv3. (For example: Shark-0012E8)
***SNMPTRAPAUTHTYPE**	Query or set the SNMP TRAP authentication type in SNMPv3. AT*SNMPTRAPAUTHTYPE? to query AT*SNMPTRAPAUTHTYPE=n to set • n=0—MD5 • n=1—SHA
***SNMPTRAPCOMMUNITY**	SNMP TRAP community string in SNMPv2 and SNMPv3. (SNMP equivalent of a password)
***SNMPTRAPDEST**	Query or set the SNMP TRAP destination in SNMPv2 and SNMPv3. (for example: 192.168.13.33)
***SNMPTRAPPORT**	• Query or set the SNMP TRAP port in SNMPv2 and SNMPv3. 1–65535 (Default is 162.)
***SNMPTRAPPRIVTYPE**	Query or set the SNMP TRAP privacy type in SNMPv3. AT*SNMPTRAPPRIVTYPE? to query AT*SNMPTRAPPRIVTYPE=n to set • n=0—DES • n=1—AES

Table D-8: Services AT Commands

Command	Description
***SNMPTRAPSECLVL**	Query or set the SNMP TRAP security level in SNMPv3. AT*SNMPTRAPSECLVL? to query AT*SNMPTRAPSECLVL=n to set • n=0—none • n=1—authentication only • n=2—authentication + privacy
***SNMPTRAPUSER**	Query or set a SNMP TRAP username string in SNMPv3.
Email (SMTP) Commands	
***SMTPADDR**	Query or set the mail server IP address or FQDN. AT*SMTPADDR? to query AT*SMTPADDR=[d.d.d.d] or [NAME] to set • d.d.d.d=IP Address • NAME=domain name (maximum: 40 characters)
***SMTPFROM**	Query or set the email address from which the SMTP message is being sent (required by some mail servers). AT*SMTPFROM? to query AT*SMTPFROM=EMAIL to set • EMAIL=email address (maximum: 30 characters)
***SMTPSUBJ**	Query or set the email subject line to use for sending emails. AT*SMTPSUBJ? to query AT*SMTPSUBJ=STRING to set
***SMTPPW**	Query or set the email server password (required by some mail servers). AT*SMTPPW? to query AT*SMTPPW=PASSWORD to set
***SMTPUSER**	Query or set the email account username (required by some mail servers). AT*SMTPUSER? to query AT*SMTPUSER=USER to set (maximum: 40 characters)
Time (SNTP) Commands	
***SNTP**	Query or set daily SNTP updates of the system time. AT*SNTP? to query AT*SNTP=n to set • n=0—Off • n=1—On
***SNTPADDR**	SNTP Server IP address, or fully-qualified domain name, to use if *SNTP=1. AT*SNTPADDR? to query AT*SNTPADDR=[d.d.d.d] or [NAME] • d.d.d.d=IP Address • NAME=FQDN

GPS

Table D-9: GPS AT Commands

Command	Description
***GPSDATA?**	Query the device and provides a snap-shot of GPS data. This command is independent of all GPS configuration. You don't need to have a server configured or any specific report type selected. The response to this command lists the fix status, satellite count, and latitude and longitude in decimal degrees. It is not formatted as a GPS report. For example: AT*GPSDATA? returns: GPS Fix=1 Satellite Count=8 Latitude=+49.17081 Longitude=-123.06970
***PGPS**	Query or set the serial streaming interface ports that the reports are sent to. AT*PGPS? to query AT*PGPS=n to set • n=0—None • n=1—DB9 Serial • n=2—USB Serial • n=3—DB9 and USB • n=4—I/O X-Card Serial • n=5—I/O X-Card Serial and DB9 • n=6—I/O X-Card Serial and USB • n=7—I/O X-Card Serial, DB9 and USB
***PGPSC**	Query or set the out-of-coverage setting. This setting enables you to configure the AirLink device to stream GPS reports to the serial port only when the device has no cellular coverage. (This enables you to use a back-up in-vehicle mapping application that does not rely on cellular network coverage. AT*PGPSC? to query AT*PGPSC=n to set • n=0: ALWAYS (default) GPS reports are always streamed to the serial port • n=1: Out of Coverage—GPS reports are only streamed to the serial port when the AirLink device has no cellular network connection. *Note: The two persistent GPS report parameters, *PGPSR and *PGPSF, control the report type and message frequency of reports sent out the serial port when the AirLink device is out of cellular network coverage.*

Table D-9: GPS AT Commands (Continued)

Command	Description
***PGPSD**	Query or set the delay (in seconds) before the out-of-coverage stream begins sending the messages out the serial port and not into SnF. AT*PGPSD? to query AT*PGPSD=n to set • n=0 (default) • n=1–255 *Note: Any messages put into SnF during this switch-over delay period are sent over the air when coverage is re-acquired.* *Note: The two persistent GPS report parameters, *PGPSR and *PGPSF, control the report type and message frequency of reports sent out the serial port when the AirLink device is out of cellular network coverage.*
***PGPSF**	Query or set how frequently (in seconds) the GPS report is sent to the serial link. AT*PGPSF? to query AT*PGPSF=n to set • n= 0–65535
***PGPSR**	Query or set the GPS report type. AT*PGPSR? to query AT*PGPSR=n to set NMEA reports: • n=E0—NMEA GGA + VTG • n=E1—NMEA GGA+VTG+RMC • n=E2—NMEA GGA+VTG+RMC+GSA+GSV TAIP reports: • n=F0—TAIP data • n=F1—TAIP compact data • n=F2—TAIP LN report • n=F3—TAIP TM report
***PPDIST** ***PP2DIST** ***PP3DIST** ***PP4DIST**	Query or set the GPS report distance interval in 100 meter units. For example, if you entered a value of 635, it would translate to 63,500 meters (63.5 kilometers). AT*PP[Server number if other than server 1]DIST? to query AT*PP[Server number if other than server 1]DIST=n to set • n=0 — Disabled • n=1–65535 — Distance in 100 meter units that the device moves before sending a GPS report

Table D-9: GPS AT Commands (Continued)

Command	Description
***PPDISTM** ***PP2DISTM** ***PP3DISTM** ***PP4DISTM**	Query or set the GPS report distance Interval in meters. AT*PP[Server number if other than server 1]DISTM? to query AT*PP[Server number if other than server 1]DISTM=n to set • n=0 — Disabled • n=100–65535—Distance in meters that the device moves before sending a GPS report *Note: If you enter a value greater than zero, but less than 100, ALEOS rounds it up to 100.*
***PPDEVID**	Query or set whether or not the RAP GPS report includes device ID and if so, which type of device ID is included. AT*PPDEVID? to query AT*PPDEVID=n to set • n=0—None • n=1—Phone number • n=2—ESN/IMEI *Note: The device ID in the RAP report is in hex, not plain text.*
***PPFLUSHONEVT**	Query or set Send SnF Buffer Immediately on input. If this feature is enabled, any pending stored reports are sent if the I/O input changes, a stationary vehicle is moved, or a maximum speed is exceeded. AT*PPFLUSHONEVT? to query AT*PPFLUSHONEVT=n to set • n=0—Disable • n=1—Enable

Table D-9: GPS AT Commands (Continued)

Command	Description
***PPGPSR** ***PP2GPSR** ***PP3GPSR** ***PP4GPSR**	Query or set the GPS report type. AT*PP[Server number if other than server 1]GPSR? to query AT*PP[Server number if other than server 1]GPSR=n to set RAP reports: • n=0 — Use legacy reports specified in *MF value. Note: Must also have *PPDEVID=0. • n=11 — Standard GPS Report • n=12 — Standard GPS Report + UTC Date • n=13 — Standard GPS Report + UTC Date + RF data • n=14—Standard GPS report + GPS + Date + RF + EIO Xora reports • n=D0 — Xora NMEA reports • n=E0 — GGA and VTG NMEA reports • n=E1 — GGA, VTG and RMC NMEA reports • n=E2 — GGA, VTG, RMC, GSA and GSV NMEA reports TAIP reports • n=F0 —TAIP data—TAIP GPS report that contains position and velocity • n=F1 —TAIP GPS report that contains the compact position • n=F2—TAIP LN report—TAIP GPS report that contains a long navigation message • n=F3—TAIP TM report—TAIP GPS report that contains the time and date
***PPINPUTEVT** ***PP2INPUTEVT** ***PP3INPUTEVT** ***PP4INPUTEVT**	Query or set ability to send a special report for digital input changes. AT*PP[Server number if other than server 1]INPUTEVT? to query AT*PP[Server number if other than server 1]INPUTEVT=n to set • n=0 — Disable • n=1 — Enable
***PPIP** ***PP2IP** ***PP3IP** ***PP4IP**	Query or set the IP address where GPS reports are sent. See also *PPPORT on page 358. AT*PP[Server number if other than server 1]IP? to query AT*PP[Server number if other than server 1]IP=d.d.d.d to set • d.d.d.d=IP address Example: AT*PPIP=192.100.100.100
***PPLATS**	Query or set the local reporting interval (in seconds). AT*PPLATS? to query AT*PPLATS=n to set • n=0—Disable (default) • n=1–255 (seconds)
***PPLATSEXTRA**	Query or set the number of additional consecutive ports that the local GPS report is sent to. AT*PPLATSEXTRA? to query AT*PPLATSEXTRA=n to set • n=0—Just the original report is sent (default). • n=1–7—Send GPS report copies to that number of ports. Example: If AT*PPLATSEXTRA=7 and the port in S53 is 1000, then GPS reports will be sent to ports 1000–1008.

Table D-9: GPS AT Commands (Continued)

Command	Description
***PPLATSR**	Query or set the GPS report type that is sent to the local client (Ethernet, USB/net, or PPP). AT*PPLATSR? to query AT*PPLATSR=n to set RAP reports: • n=11—GPS Data • n=12—GPS + Date • n=13—GPS + UTC + RF • n=14—GPS + Date + RF + EIO NMEA reports: • n=E0—NMEA GGA + VTG • n=E1—NMEA GGA + VTG + RMC • n=E2—NMEA GGA + VTG + RMC + GSA + GSV TAIP reports: • n=F0 —TAIP data—TAIP GPS report that contains position and velocity • n=F1 —TAIP GPS report that contains the compact position • n=F2—TAIP LN report—TAIP GPS report that contains a long navigation message • n=F3—TAIP TM report—TAIP GPS report that contains the time and date
***PPMAXRETRIES** ***PP2MAXRETRIES** ***PP3MAXRETRIES** ***PP4MAXRETRIES**	Query or set maximum number retries when in Simple Reliable mode, UDP Sequence mode, and TCP transports. AT*PP[Server number if other than server 1]MAXRETRIES? to query AT*PP[Server number if other than server 1]MAXRETRIES=n to set • n=0—Disabled • n=1–255 retries (Maximum is 10.)
***PPMINTIME** ***PP2MINTIME** ***PP3MINTIME** ***PP4MINTIME**	Query or set the minimum amount of time between report packets. Each packet can contain multiple reports. This is useful to limit network traffic and make more efficient use of bandwidth. You can also use it in conjunction with store and forward. The minimum value depends on the policies of the Mobile Network Operator. AT*PP[Server number if other than server 1]MINTIME? to query AT*PP[Server number if other than server 1]MINTIME=n to set • n=0—Disable • n=1–65535 seconds
***PPODOM** ***PP2ODOM** ***PP3ODOM** ***PP4ODOM**	Query or set including the current odometer reading in the RAP report. AT*PP[Server number if other than server 1]ODOM? to query AT*PP[Server number if other than server 1]ODOM=n to set • n=0—Disabled (default) Do not include odometer reading in report. • n=1—Enabled Include odometer reading in report.
***PPODOMVAL**	Query or set the odometer value (in meters). Maximum value is approximately 4.3 billion meters (2.7 million miles). AT*PPODOMVAL? to query AT*PPODOMVAL=n to set • n=0–4294967295 meters

Table D-9: GPS AT Commands (Continued)

Command	Description
***PPPORT** ***PP2PORT** ***PP3PORT** ***PP4PORT**	Query or set the port GPS reports are sent to. AT*PP[Server number if other than server 1]PORT? to query AT*PP[Server number if other than server 1]PORT=n to set • n=0—Disable • n=1–65535
***PPREPORTINPUTS** ***PP2REPORTINPUTS** ***PP3REPORTINPUTS** ***PP4REPORTINPUTS**	Query or set input reporting and including the current digital input value in RAP reports. AT*PP[Server number if other than server 1]REPORTINPUTS? to query AT*PP[Server number if other than server 1]REPORTINPUTS=n to set • n=0—Disabled • n=1—Enabled
***PPSIMPLETO** ***PP2SIMPLETO** ***PP3SIMPLETO** ***PP4SIMPLETO**	Query or set the first retry interval for Simple Reliable, UDP Sequence mode, and TCP transports (in seconds). AT*PP[Server number if other than server 1]SIMPLETO? to query AT*PP[Server number if other than server 1]SIMPLETO=n to set • n=0—Disable • n=1–255 (Default is 10.)
***PPSNF** ***PP2SNF** ***PP3SNF** ***PP4SNF**	Query or set the Store and Forward (SNF) setting. SNF causes GPS reports to be stored if the device/vehicle goes outside the area of network coverage. Once the vehicle is in the coverage area, the GPS reports are sent en masse to the server. AT*PP[Server number if other than server 1]SNF? to query AT*PP[Server number if other than server 1]SNF=n to set • n=0—Disabled • n=1—Enabled (default)
***PPSNFR** ***PP2SNFR** ***PP3SNFR** ***PP4SNFR**	Query or set Transport /SNF mode. GPS reports are retransmitted if not acknowledged by the server. AT*PP[Server number if other than server 1]SNFR? to query AT*PP[Server number if other than server 1]SNFR=n to set • n=0—Disabled • n=1—Reliable mode • n=2—Simple Reliable mode • n=3—UDP Sequence • n=4—TCP Listen • n=5—TCP
***PPTAIPID**	Query or set the four character alphanumeric TAIP ID. AT*PPTAIPID? to query AT*PPTAIPID=nnnn to set • nnnn=alphnumeric characters

Table D-9: GPS AT Commands (Continued)

Command	Description
***PPTIME** ***PP2TIME** ***PP3TIME** ***PP4TIME**	Query or set the GPS report time interval (in seconds). AT*PP[Server number if other than server 1]TIME? to query AT*PP[Server number if other than server 1]TIME=n to set • n=0 – 65535 seconds *Note: Your cellular Mobile Network Operator may impose a minimum transmit time.* See also *PPMINTIME, *PPTSV, +CTA. *Note: A report time of less than 30 seconds may keep an RF link up continuously, tying up an RF resource to transfer small amounts of data. Generally, the RF channel is released and goes dormant in 10–20 seconds if no data is sent or received.*
***PPTCPPOLL**	Query or set the port to listen on for TCP GPS report polling. *Note: The request to this port needs to come from the same IP address in *PPIP on page 356 and uses the report type configured for server 1.* AT*PPTCPPOLL? to query AT*PPTCPPOLL=n to set • n=0—Disabled • n=1–65535 (default 9494)
***PPTSV** ***PP2TSV** ***PP3TSV** ***PP4TSV**	Query or set the time interval in minutes that the device sends in reports when it is stationary (Stationary vehicle timer). AT*PP[Server number if other than server 1]TSV? to query AT*PP[Server number if other than server 1]TSV=n to set • n=0—Disabled • n=1–255 minutes For example, if *PPTIME=10, the device sends GPS reports at least once every 10 seconds while it is moving; however, once it stops moving, it slows the reports down to this *PPTSV value. *Note: In order for the PPTSV (Stationary Vehicle timer) to take effect, the PPTIME value must be set to a value greater than 0 and less than the PPTSV value. The PPTSV timer checks for vehicle movement at the PPTIME interval, so if PPTIME is disabled, then PPTSV will also be disabled.*

Serial

If you have a GX Series device with an I/O X-Card installed, you can execute many of the serial commands “as is” in a terminal session connected to the specific port for which the command is intended. However, you can explicitly specify which port the command takes effect on by adding a port identifier to the end of the full command.

If you use the command alone (without the “comma port identifier”) from any non-serial terminal session (for example, telnet), the command takes effect on the main port on the device.

Examples:

ATAIP=1 when executed in a terminal connected to the I/O X-Card serial port, sets the Allow IP Address for the X-Card's serial port.

ATAIP=1,0 when executed in a terminal connected to the I/O X-Card serial port sets the Allow IP Address for the serial port on the device port.

ATAIP=0,1 when executed in a terminal connected to the serial port on the device sets the Allow IP Address for the X-Card's serial port.

ATAIP=0 when executed in a telnet session sets the Allow IP Address for the device's serial port.

Table D-10: Serial AT Commands

Command	Description
AIP	Query or set the option to allow IP addresses to communicate on UDP over serial. AT*AIP? to query AT*AIP=n to set • n=0 — Allow only the IP address specified in S53 to connect when UDP auto answer is enabled (S82=2) • n=1 — Allow any incoming IP address to connect when UDP auto answer is enabled (S82=2) Always subject to any security filters that may be defined. (See Security on page 344.)
\APPP	Initiates a PPP connection on serial terminal. You can also initiate a PPP connection using the ADT command and one of the supported phone numbers. *Note: PPP is not available on the I/O X-Card serial port.*
***CTSE**	Query or set asserting Clear To Send (CTS) when there is a network coverage. AT*CTSE? to query AT*CTSE=n to set • n=0 — Disabled (Default) • n=1 — Enable assertion of CTS when there is network coverage
DAE	Query or set AT Escape Sequence detection. ATDAE? to query ATDAE=n to set • n=0 — Enable • n=1 — Disable (The escape sequence (+++) is ignored.)
***DPORT**	Query or set the device port that the device listens on for inbound packets/data/polls. AT*DPORT? to query AT*DPORT=n to set • n=1–65535

Table D-10: Serial AT Commands (Continued)

Command	Description
***DU**	Query or set the dial command to only use UDP. AT*DU? to query AT*DU=n to set • n=0 — Dial using the means specified (default) • n=1 — Dial UDP always, even when using ATDT When this parameter is set you cannot establish a TCP PAD connection by using the Dial command.
***ENQ**	Query or set the option to output an ENQ [0x05] after the TCP CONNECT, delayed by the Delay Connect Response time (S221). AT*ENQ? to query AT*ENQ=n to set • n=0 — Disable (Default) • n=1 — Enable ENQ on TCP CONNECT
***HOSTMODE?**	Query the current host mode. AT*HOSTMODE? returns: • AT • PPP • TCP • UDP *Note: If the device is not in AT mode, Telnet into the device to execute this command.*
MD	Query or set the default start-up mode for the serial port. When the device is power-cycled, the serial port enters the mode specified by this command after 5 seconds. On startup, typing ATMD0 within 5 seconds changes the mode to normal (AT command) mode. See also S53 to set the port for UDP. AT*MD? to query AT*MD=hh to set • hh (hex byte)=00 — Normal (AT Command mode) • hh=02 — PPP • hh=03 — UDP • hh=04 — TCP • hh=08 — reverse telnet/ssh • hh=13 — Modbus ASCII • hh=23 — Modbus RTU (Binary) • hh=33 — BSAP • hh=63 — Variable Modbus • hh=83 — UDP Multiple Unicast *Note: The I/O X-Card only supports AT, UDP, and TCP.*

Table D-10: Serial AT Commands (Continued)

Command	Description
MLIST	Add IP addresses to the Modbus address list or query the Modbus address list, using decimal index values. Format is MLISTIndex(decimal)=IP address Example: ATMLIST10=123.123.123.123, where: • 10 is the Index • 123.123.123.123 is the IP address MLISTIndex=IP to add an IP address to the list Including the port number after the IP address is optional. If you include the port number, separate the port number and IP address by a colon. For example: 10=123.123.123.123:11223 MLIST? to query the Modbus address list; returns the addresses in the list in the format Index=IP. For example: 10=123.123.123.123 11=124.124.124.124 12=125.125.125.125 13=126.126.126.126 Range for index numbers is 0—65535. The Modbus address list accepts up to 100 entries. *Note: This command is not supported on the I/O X-Card serial port.*
MLISTX	Add IP addresses to the Modbus address list or query the Modbus address list, using hexadecimal index values. Format is MLISTXIndex(hex)=IP address Example: ATMLISTX000A=123.123.123.123, where: • 000A is the Index • 123.123.123.123 is the IP address MLISTXIndex=IP to add an IP address to the list Including the port number after the IP address is optional. If you include the port number, separate the port number and IP address by a colon. For example: 0xA=123.123.123.123:11223 MLISTX? to query the Modbus address list returns; returns the addresses in the list in the format Index=IP. For example: 000A=123.123.123.123 000B=124.124.124.124 000C=125.125.125.125 000D=126.126.126.126 Range for index numbers is 0—FFFF. The Modbus address list accepts up to 100 entries. *Note: This command is not supported on the I/O X-Card serial port.*
MVLEN	Query or set the length of the Modbus Variant ID. ATMVLEN? to query ATMVLEN=[length of the RTU ID in bytes] to set *Note: This command is not supported on the I/O X-Card serial port.*

Table D-10: Serial AT Commands (Continued)

Command	Description
MVMSK	Query or set the Modbus Variant ID Mask (byte hex mask to use when extracting the ID). This parameter is used when the when the Mode Default (MD on page 361) is set to hex 63. ATMVMSK? to query ATMVMSK=[byte hex mask] to set *Note: This command is not supported on the I/O X-Card serial port.*
MVOFF	Query or set the Modbus (Variable mode) offset in the data where the Modbus ID starts. ATMVOFF? to query ATMOFF=n to set • n= 0–255 *Note: This command is not supported on the I/O X-Card serial port.*
MVTYP	Query or set the Modbus Variant type (RTU ID data-type in a modbus-variant protocol). This parameter is used when MD on page 361 is set to 63. It defines the data-type of the RTU ID in Modbus-like protocol data packets. ATMVTYP? to query ATMVTYP=n to set • n=0—Binary • n=1—ASCII hex • n=2—ASCII decimal *Note: This command is not supported on the I/O X-Card serial port.*
IPL	Query or set the IP list dial. AT*IPL? to query AT*IPL=n to set • n=0—Disable • n=1—Enable This allows you to access to the Modbus IP address list using the first two digits of the dial string. Example: ATDT1234567 would go to ID “12” on the Modbus list and use the associated IP as the destination.
***NUMTOIP**	Query or set the option to convert a 12-digit number to an IP address For example, converts 111222333444 to 111.222.333.444 AT*NUMTOIP? to query AT*NUMTOIP=n to set • n=0—Disable • n=1—Enable

Table D-10: Serial AT Commands (Continued)

Command	Description
S50	Query or set the data forwarding idle time-out. ATS50? to query ATS50=n to set • n=0 — a forwarding time-out of 10ms is used. • n= tenths of a second
S51	Query or set the PAD data forwarding character. ASCII code of character that causes data to be forwarded. Used in UDP or TCP PAD mode. ATS51? to query AT51=CHARACTER to set • n=0 — No forwarding character • n= CHARACTER
S53	Query or set the method (dial mode), destination IP address, and port used as defaults for the D (Dial) AT command. ATS53? to query ATS53=[method][d.d.d.d][/ppppp] to set [method] can be: • P — UDP • T — TCP [d.d.d.d] is the destination IP address [pppp] is the port number. Example: ATS53=P111.22.33.44/5555 where: • The first character is the dial mode (P in this example) • Followed by destination IP address (111.22.33.44 in this example) • A slash • Followed by the destination port (5555 in this example) You can also use this command to set only the port. For example, AT53=/7777.
S60	Query or set the Telnet Client Echo Mode. ATS60? to query ATS60=n to set • n=0 — No Echo • n=1 — Local Echo (Default) • n=2 — Remote Echo
S82	Query or set UDP auto answer. ATS82? to query ATS82=n to set • n=0 — Disable • n=1 — Enable

Table D-10: Serial AT Commands (Continued)

Command	Description
S83	Query or set the UDP auto answer idle time-out. If no data is sent or received before the time-out occurs, the current UDP session is terminated. While a session is active, packets from other IP addresses are discarded (unless *UALL is set). ATS83? to query ATS83=n to set • n=0 — No idle time-out (Default) • n=1 – 255 — Time-out in seconds
TCPS	Query or set the TCP connection time-out (TCPS) units. If there is no traffic through the TCP connection for the specified interval, the connection is terminated. AT*TCPS? to query AT*TCPS=n to set • n=0 — minutes • n=1—seconds
TCPT	Query or set the interval to terminate a TCP connection when there s no traffic. This value affects only the TCP connection in TCP PAD mode. AT*TCPT? to query AT*TCPT=n to set • n=0–255
***UALL**	Query or set the ability to accept UDP packets from any IP address when a UDP session is active. If there is no UDP session active, an incoming UDP packet will be treated according to the UDP auto answer and AIP settings. AT*UALL? to query AT*UALL=n to set • n=0 — No effect (Default) • n=1 — Accept UDP data from all IP addresses when in a UDP session
***UDPLAST**	Query or set the option to set S53 to the last accepted IP address through UDP auto answer. This can be used in conjunction with MD3 so that when there is no UDP session, new Ethernet host data will cause a connection to be restored to the last IP accepted through UDP auto answer. AT*UDPLAST? to query AT*UDPLAST=n to set • n=0 — Does not change destination IP (default) • n=1 — Change destination IP to last received
***USD**	Query or set the specified delay before sending the UDP packets out the serial port. AT*USD? to query AT*USD=n to set • n=0 — No UDP packet delay (Default) • n=1 – 255 — Delay in 100ms units, from 100 ms to 25.5 sec.

Standard (Hayes) commands

The following table contains Hayes commands supported on AirLink devices.

Table D-11: Standard (Hayes) AT Commands

Command	Description
+++	AT escape sequence (not preceded by AT) If a serial terminal is in a data mode, typing this sequence on that serial terminal causes the terminal to re-enter AT command mode. There must be an idle time on the serial port before and after the sequence. The idle time is set by the value in S50. After you type the AT escape sequence, the terminal remains in AT command mode for 15 seconds before it automatically leaves AT command mode and returns to the previous data mode. *Note: The "+" is ASCII character 0x2B.* *Note: The detection of this sequence is disabled if DAE=1.*
&C	Query or set Data Carrier Detect (DCD) mode. DCD is a hardware signal that notifies the software that the device is communicating with another device. AT&C? to query AT&Cn to set • n=0 — Always assert DCD • n=1 — Assert DCD enable when network is ready (default) If you have a GX Series device with an I/O X-Card installed, you can query or set the main port on the device or the port on the X-Card by specifying the port number. If no port is specified, the query or command affects the port your are telnetting to. AT&C?,[p] to query AT&Cn,[p] to set • p=0—Main serial port on the device • p=1—Serial port on the I/O X-Card *Note: Do not use an equal sign (=) when issuing the command.*

Table D-11: Standard (Hayes) AT Commands (Continued)

Command	Description
D[*method*] [*d.d.d.d*] [*/ppppp*] **or** **D[*method*] [[@]*name*] [*/ppppp*]**	Dial a connection to a remote IP and Port using either UDP, TCP, or Telnet. *method* = P — Establish a UDP connection T — Establish a TCP connection N — Establish a Telnet connection *d.d.d.d* = IP address to establish connection to *name* = Domain name to establish connection to *ppppp* = IP port to establish connection to Examples: **ATD** — Dial (establish) default connection per **S53** **ATDP***nnn.nnn.nnn.nnn*[/ppppp] — Dial (establish) UDP session to the specified IP address/port. If the method, IP address, or port is omitted, the values from S53 are used. If a Telnet connection is requested (N) and the port is not supplied, port 23 will be used instead of the value from S53. Several special dialing numbers exist to make it easy to establish a **PPP** connection with the device. **ATD#19788** or **ATDT#19788** will establish a PPP connection (see \APPP on page 360). If a domain name is specified, the '@' symbol can be used to explicitly indicate the start of the name. For example, if "**ATDPHONY**" is issued, this will be interpreted as dial a UDP connection to "HONY". To dial using the default method to host "PHONY", one would issue "ATD@PHONY". To end the connection, issue the **+++** escape sequence or drop the DTR line (if Ignore DTR **S211=0** or **&D2**). *Note: The source port of the session is the **Device Port** (set by ***DPORT**).*
&D	Query or set Data Terminal Ready (DTR) mode. AT&D? to query AT&Dn to set • n=0 — Devices ignores DTR, same effect as HW DTR always asserted (same as S211=1); DTD is assumed to be on. • n=1 — DRT drop causes the device to switch to AT command mode, but does not drop the connection. • n=2 — DTR drop causes the connection to drop. • n=3—DTR drop causes the connection to reinitialize. If you have a GX Series device with an I/O X-Card installed, you can query or set the main port on the device or the port on the X-Card by specifying the port number. If no port is specified, the query or command affects the port your are telnetting to. AT&D?,[p] to query AT&Dn,[p] to set • p=0—Main serial port on the device • p=1—Serial port on the I/O X-Card *Note: Do not use an equal sign (=) when issuing the command.*

Table D-11: Standard (Hayes) AT Commands (Continued)

Command	Description
***DATZ**	Query or set the option to block device reset using ATZ. AT*DATZ? to query AT*DATZ=n to set • n=0 — Off. Block is disabled—ATZ resets the device. (default) • n=1 — On. Block is enabled—ATZ does not reset the device.
E	Toggle AT command echo mode. ATE? to query ATEn to set • n=0 — Echo Off; does not echo commands to the computer • n=1 — Echo On; echoes commands to the computer (so you can see what you type) *Note: Do not use an equal sign (=) when issuing the command.*
H	ATH hangs up, immediately terminates the session (PAD or PPP).
HOR	Half-Open Response — In UDP auto answer (half-open) mode. AT*HOR? to query AT*HOR=n to set • n=0 — No response codes when UDP session is initiated • n=1 — RING CONNECT response codes sent out serial link before the data from the first UDP packet *Note: Quiet Mode must be Off.*
Q	Query or set AT quiet-mode. If quiet mode is set, there is no responses to AT commands except for data queried. ATQ? to query ATQn to set • n=0 — Off (Default) • n=1 — Quiet-mode on *Note: Do not use an equal sign (=) when issuing the command.*

Table D-11: Standard (Hayes) AT Commands (Continued)

Command	Description
\Q	Query or set the serial port flow control. AT\Q? to query AT\Qn to set • n=0 — No flow control • n=1 — Hardware flow control • n=4 — Transparent software flow control If you have a GX Series device with an I/O X-Card installed, you can query or set the main port on the device or the port on the X-Card by specifying the port number. If no port is specified, the query or command affects the port your are telnetting to. AT\Q?,[p] to query AT\Qn,[p] to set • p=0—Main serial port on the device • p=1—Serial port on the I/O X-Card *Note: Do not use an equal sign (=) when issuing the command.*
&S	Query or set DSR. AT&S? to query AT&Sn to set • n=0—Always assert • n=1—Assert DSR while in data mode (UDP, TCP, PPP) If you have a GX Series device with an I/O X-Card installed, you can query or set the main port on the device or the port on the X-Card by specifying the port number. If no port is specified, the query or command affects the port your are telnetting to. AT&S?,[p] to query AT&Sn,[p] to set • p=0—Main serial port on the device • p=1—Serial port on the I/O X-Card *Note: Do not use an equal sign (=) when issuing the command.*
S0	Query or set TCP auto answer (the number of rings required before the device automatically answers a call). ATS0? to query ATS0n to set • n=0— Disable • n=1—Enable *Note: Do not use an equal sign (=) when issuing the command.*

Table D-11: Standard (Hayes) AT Commands (Continued)

Command	Description
S23	Configure Serial Port ATS23? to query ATS23=[speed],[data bits][parity][stop bits] to set Speed: • 300 • 1200 • 2400 • 4800 • 9600 • 19200 • 38400 • 57600 • 115200 Data bits: • 7 • 8 Parity: • O=Odd • E=Even • N=None • M=Mark Stop bits: • 1 • 1.5 • 2 Example: ATS23=115200,8N1 (Sets the device to 115200, etc.) The settings take effect after reset. *Note: Must be 8 data bits for PPP mode.*
S211	For applications or situations where hardware control of the DTR signal is not possible, the device can be configured to ignore DTR. When Ignore DTR is enabled, the device operates as if the DTR signal is always asserted. ATS211? to query ATS211=n to set • n=0—Use hardware DTR (default) • n=1—Ignore DTR • n=3—Ignore DTR and assert DSR.
S221	Query or set the Connect Delay—the number of seconds to delay the connect response when establishing a TCP connection. ATS211? to query ATS211=n to set • n=0–255

Table D-11: Standard (Hayes) AT Commands (Continued)

Command	Description
V	Query or set the AT command responses (verbosity). ATV? to query ATVn to set • n=0 — Numeric (terse) command responses (The numeric responses follow the Hayes Standards for commands.) • n=1 — Text string (verbose) command responses (default) *Note: Do not use an equal sign (=) when issuing the command.*
&V	Lists most AT commands and their current values. If the parameter is not configured, the AT command returns “Not Set”.
&W	Saves the settings for parameters that are temporarily set without being permanently written to the memory. This command does not apply to ALEOS because once you issue an AT command or change a setting in ACEmanager and click Apply, the changes are saved in non-volatile memory and are persist across reboots.
X	Query or set the Extended Call Process Result mode ATX? to query ATXn to set • n=0 — No extended code (default) • n=1 — Adds the text 19200 to the connect response
Z	Reboots the AirLink device. *Note: If *DATZ is set to 1, Z is blocked. See *DATZ on page 368.*

I/O

Table D-12: Input/Output AT Commands

Command	Description
***ANALOGIN[n]?**	Query individual analog input values (in volts). AT*ANALOGIN[n]? • n=1–4 *Note: Four analog inputs are available on an AirLink GX Series device with an I/O X-Card installed. To confirm that an I/O X-Card is installed, check the X-Card Type field on Status > Home.* *One analog input is available on the AirLink LS300.*

Table D-12: Input/Output AT Commands (Continued)

<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td>*DIGITALIN[n]?</td><td>Query individual digital inputs. The digital inputs report either a 0 (open) or 1 (closed).
AT*DIGITALIN[n]?
• n=1–5 (Input number)

<table><tr><th>Volts</th><th>Digital value</th></tr><tr><td>-0.5–1.2</td><td>0</td></tr><tr><td>1.3–30</td><td>1</td></tr></table>
Note: Digital inputs 2, 3, 4, and 5 are only available on an AirLink GX Series device with an I/O X-Card installed. To confirm that an I/O X-Card is installed, check the X-Card Type field on Status > Home.</td></tr>
<tr><td>*PULSECNT[n]?</td><td>Query the I/O pulse counts for digital in.
AT*PULSECNT[n]?
• n=1–5

Note: Pulse counts 2–5 are only available on a GX Series device with an I/O card installed.</td></tr>
<tr><td>*RELAYOUT[#]</td><td>Query or set the relay status.
AT*RELAYOUT[#]? to query
AT*RELAYOUT[#]=n to set
• # = 1–5
• n=0—OFF
• n=1—Drive Active Low

Note: Relay outputs 3, 4, and 5 are only available on an AirLink GX Series device with an I/O X-Card installed. To confirm that an I/O X-Card is installed, check the X-Card Type field on Status > Home.</td></tr>
</table>

Applications

Table D-13: Applications > Data Usage Commands

Command	Description
***DATACURDAY?**	Display data usage for the current day (in KB).
***DATAPLANUNITS**	Query or set the units for the data usage report AT*DATAPLANUNITS to query AT*DATAPLANUNITS=n to set • n=1—Sets the units to Megabytes (MB) • n=2—Sets the units to Kilobytes (KB)

Table D-13: Applications > Data Usage Commands

Command	Description
***DATAPREVDAY?**	Query the data usage for the previous day (in KB).
***DATAUSAGEENABLE**	Query or set enabling Data Usage. AT*DATAUSAGEENABLE? to query AT*DATAUSAGEENABLE=n to set • n=0—Data Usage disabled • n=1—Data Usage enabled
***GARMINATTACH**	Query or set the ability to connect a Garmin device to the serial port (so the Garmin device can communicate with a remote server). For more information, see Garmin on page 248. AT*GARMINATTACH? to query AT*GARMINATTACH=n to set • n=0—Disable • n=1—Enable
***GARMINSTATUS?**	Query Garmin device attachment status.

Admin

Table 4-14: Admin > Advanced Commands

Command	Description
***BLOCK_RESET_CONFIG**	Query or set the ability to block resetting the device to factory default settings using the hardware Reset button. AT*BLOCK_RESET_CONFIG? to query AT*BLOCK_RESET_CONFIG=n to set • n=0—Reset button can be used to reset the device to factory default settings. (default). • n=1—Device cannot be reset to factory default settings using the Reset button on the device. *Note: This command only blocks the ability to reset to defaults using the Reset button on the device. You can still reset the device to the factory default settings using the "Reset to Factory Default" button in ACEmanager or the *RESETCFG AT command.*
***BOARDTEMP?**	Query the temperature of the internal hardware, in degrees Celsius.
***DATE?**	Query the internal clock. The date and time are always specified in a 24-hour notation. AT*DATE? to query *Note: In AirLink devices, the GPS and/or cellular connection is used to set the time.*

Table 4-14: Admin > Advanced Commands

Command	Description
***MSCIUPADDR**	Query or set the IP address or FQDN and port that periodic device status updates are sent to. AT*MSCIUPADDR[IP address or FQDN][/port]? to query AT*MSCIUPADDR=[IP address or FQDN][/port] to set Examples: 192.168.14.100/3333 MyDevice.com/3333
***MSCIUPDPERIOD**	Query or set the device status update interval (in seconds). Thsi specifies how frequently the device status update is sent to the port configured in *MSCIUPADDR. AT*MSCIUPDPERIOD? to query AT*MSCIUPDPERIOD=n to set • n=0 — Disabled • n=1–255 seconds
NSLOOKUP	Immediately performs an NSLookup on the supplied FQDN. ATNSLOOKUP=[FQDN]
***POWERIN?**	Query the voltage input to the internal hardware.
***RESETCFG**	AT*RESTCFG resets the device to factory default settings. **Important:** *There is no confirmation requested. The AT command takes effect immediately.*
***REMOTELOG**	Exports the log file to a remote destination (Syslog Server). Specifying the port is option. If the port is not specified, the default port, 514, is used. AT*REMOTELOG=SYSLOG SERVER IP,PORT

***SECUREMODE**	Query or set the secure mode that blocks most ports (and ICMP) for over-the-air (OTA) or OTA and local to prevent unwanted access to the device.
	AT*SECUREMODE? to query
	AT*SECUREMODE=n to set
	• n=0 Off; normal behavior
	• n=1 Disables:
	  • Web management ports (ACEmanager and AVMS access) from the OTA interface
	  • Internet Control Message Protocol (ICMP), used for PING, for OTA and Wi-Fi
	• n=2 Disables:
	  • Web management ports from the Over-the-air (OTA) interface
	  • Internet Control Message Protocol (ICMP) for OTA and Wi-Fi
	  • ICMP for local ports (Ethernet, USB, and Serial)
	Note: Telnet and SSH ALEOS ports remain open regardless of the secure mode setting. This enables you to connect an AT console to manage the device. DHCP and DNS ports also remain open to allow the device to provide IP addresses to hosts and relay the DNS service.

Table 4-14: Admin > Advanced Commands

Command	Description
***SYSRESETS?**	Query the number of resets since the device was reset to factory default settings.
***USBBYPASS**	Query or set Radio Passthru mode. AT*USBBYPASS? to query AT*USBBYPASS=n to set • n=0—Disable • n=1—Enable

E: SMS Commands

SMS Command format

PW [Password] [Prefix][Command or Command parameter1] [Command parameter2 (if applicable)] [Command parameter n]

Note: There is no space between the prefix and the command (or the 1st command parameter in the case of multi-parameter commands). There must be a single space between all other fields to act as a delimiter.

The default password is the last 4 digits of the SIM ID number (for SIM-based devices) and the last 4 digits of the ESN (for non-SIM devices). If you do not know the SIM ID or ESN number, you can find it in ACEmanager on the Status > WAN/Cellular page.

The default prefix is “&&&”.

Whether or not a password and prefix are required varies depending on the SMS mode selected in ACEmanager.

SMS mode	Password (configurable in all modes)	Prefix
Password Only	Always required	Required Use default (not configurable)
Control Only	Required when sending from a non-trusted phone number	Prefix is configurable. The prefix can be omitted if the ALEOS Command Prefix field in ACEmanager (Services > SMS) is configured to be blank.
Gateway Only	Always required	Required Use default (not configurable)
Control and Gateway	Required when sending from a non-trusted phone number	Required Configurable, but cannot be blank

When an SMS command is received, the AirLink device performs the action requested and sends a response back to the phone number from which it received the SMS.

For more examples and detailed instructions, see SMS on page 157.

List of SMS Commands

Command	Action	Result
Note: Some responses start with "reply from [device name]:" However, this feature is currently unavailable for the Enable, GPS, Provision, AVMS, and AVMSCHECKIN commands.		
[prefix]enable <value>	Enable/disable the device(s) being managed by AVMS.	"AVMS enable set to status:" <value> <value>=0 Disable <value>=1 Enable
[prefix]status	None	status IP [Network IP] [Network Status]: [technology type] RSS signalled Lat = [Latitude] Long = [Longitude] Time = [hh:mm:ss]
[prefix]reset	Resets the device 30 seconds after the first response message is sent.	First message: Reset in 30 seconds Second message: Status message when back up.
[prefix]relay x y	Sets the applicable relay to the desired setting.	relay x set to y x can be 1 y can be 0 or 1 (Off or Drive active low)
[prefix]GPS	The device replies with its current GPS location.	The device sends a link to a map showing its location. You can copy the link into a browser to view the location, or if the SMS is sent from a smartphone, you can click the link to view the map.
[prefix]Provision <APN> <Network User ID> <Network Password> *Note: You can omit any of the above fields by using a leading or single period (.) for that parameter.* *Note: Use of this command is valid for LTE, HSPA, and GPRS networks, but not valid for CDMA only networks.*	After the unit is installed and the SIM card inserted, you can use this command to provision the account.	"provision" "apn:" <APN> "user ID" <Network User ID> "PW" <Network Password>

Command	Action	Result
[prefix]AVMS <server> <interval> *Note: All of the above must be on a single line. The interval must be greater than 0. Omitting any field results in a response of "not set" and the configuration parameter does not change.*	Modifies the AVMS server's URL and AVMS communication period (interval in minutes)	"AVMS" "srv:" <Server> "interval:" <Interval>
[prefix]AVMSCHECKIN	Prompts the device to communicate with the AVMS server. Once AirVantage Management Service receives the heartbeat message, it can respond and send an MSCI command to the device (i.e Write/Read/ Firmware Update).	"AVMS connection requested"

F: Q & A and Troubleshooting

F

ACEmanager Web UI

The ACEmanager window is not displaying properly.

1. Ensure the you are using a supported browser. See page 17 for a list of supported browsers.
2. Hold the Shift key + click the Refresh button. This reloads the page, while ignoring what is in the cache.

If the problem persists:

- Clear the cache. (The procedure varies, depending on the browser.)
- Restart the browser.
- Restart your computer.

Ethernet Ports

My GX Series device has a Ethernet X-Card installed, but the ports are not working, and the Ethernet LEDs are not lit.

1. Launch ACEmanager.
2. Go to the LAN tab.
3. Select DHCP/Addressing in the menu on the left of the screen.
4. In the Host Connection Mode field, ensure that Ethernet Uses Public IP is not select.

If “Ethernet Uses Public IP” is selected in the Host Connection Mode field, the Ethernet ports are disabled.

What do the LEDs above the Ethernet port mean?

There are two LEDs at the top of the Ethernet port. The green on is lit when there is a cable connected to the host and the connection is running at 100baseT. The amber (activity) LED blinks when traffic is passing through the port.

LAN Networks

The server on my LAN network is receiving data from some hosts on the network, but not others. What’s wrong?

If you have a network with multiple LAN hosts that are sending data to the same server and the server is not receiving data from one (or more) of the hosts, it may be because the Mobile Network Operator has a WAN firewall that is blocking the ports used by the NAT for over-the-air (OTA) destinations.

To correct this problem:

1. Launch ACEmanager.
2. Go to the LAN/WiFi tab.
3. Select Ethernet.
4. Refer to the instructions for setting the Starting Ephemeral Port on page 76.)

Wi-Fi

My GX Series device has a Wi-Fi X-Card installed, and I have it configured to act as an access point, but I don't see an option to use WEP encryption.

1. Launch ACEmanager.
2. Go to the LAN/WiFi tab.
3. Select WiFi.
4. In the Enable Access Point field, change the value from "b/g/n Enabled" to "b/g Enabled".

   Once this change is made, an "Open WEP" section appears below the WiFi Configuration section.

WEP encryption is only supported on 802.11b and 802.11g. It is not supported on 802.11n.

Port Forwarding

I set up port forwarding rules. I did not receive an error message, but it seems that data is not being forwarded.

If the Public Start Port and Public End Port fields are not set up correctly, data is not forwarded.

1. In ACEmanager, go to Security > Port Forwarding.

- If you are forwarding data to a single port:
  - Ensure that the value in the Public Start Port field is **not** 0.
  - Ensure that the value in the Public End Port field **is** 0.
  - Ensure that the value in the Private Port start field is **not** 0.
- If you are forwarding data to a range of ports:

1. Ensure that the value in the Public Start Port field is not 0.
   - Ensure that the value in the Public End Port field is greater than the value in Public Start Port field.
   - Ensure that the value in the Private Port Start field is not 0.

For complete instructions, see Port Forwarding on page 133.

ALEOS Application Framework (ALEOS AF)

I'm unable to load an application from ALEOS AF.

1. In ACEmanager, go to Services > Telnet/SSH.
2. In the AT Server Mode field, select Telnet.
3. Click Apply.
4. Re-try loading the application from ALEOS AF.

SMS

I tried to send an SMS message, and received an error code. What does the error code mean?

The following acknowledgment error codes may appear if your message was not successfully sent:

Code:	Explanation:
100	Not in coverage (no cellular service)
201	Parse Error on field #1 (Start Field)
202	Parse Error on field #2 (Phone number and separator)
203	Parse Error on field #3 (Data type and separator)
204	Parse Error on field #4 (Payload length and separator)
205	Parse Error on field #5 (Message and End Field)
301	No buffers available
302	SMS queue full

Supported SMS data types are ASCII, 8-bit, and Unicode, and are all case-sensitive. SMS messages being sent MUST be in ASCII hex format.

I tried to send an SMS command and received the error "not set". The parameter was not changed.

Check the format of the SMS command. There should be no space between the prefix and the command (or the 1st command parameter in the case of multi-parameter commands), and a single space between all other fields to act as a delimiter. For more information, see SMS Commands on page 377 and SMS on page 157.

GPS

I set the GPS Reports Port field on the GPS > Local Streaming window to stream GPS data to a USB port, but I don't see GPS data on the USB port.

The GPS streaming feature works with serial devices. To stream data to a USB port, you must first configure the USB port to act as a serial device.

1. In ACEmanager, go to the LAN > USB tab.
2. In the USB Device Mode field, select USB Serial.
3. Click Apply.

If you have not already done so:

1. Go to GPS > Local Streaming.
2. In the GPS Reports port field, select one of the following:
   - USB Serial
   - DB9 and USB
3. Click Apply.
4. After you have made all the configuration changes, reboot the device.

Error Reporting

I set up ACEmanager to send an email/SMS report, but when I clicked the Test report button no report was sent.

After you set up the error reporting fields and click Apply, wait about a minute before you click the Test report button. The AirLink device needs this time to apply the new configuration.

VPN

I followed the instruction for setting up an SSL tunnel for a VPN, including loading the root certificate, but I cannot connect to the VPN.

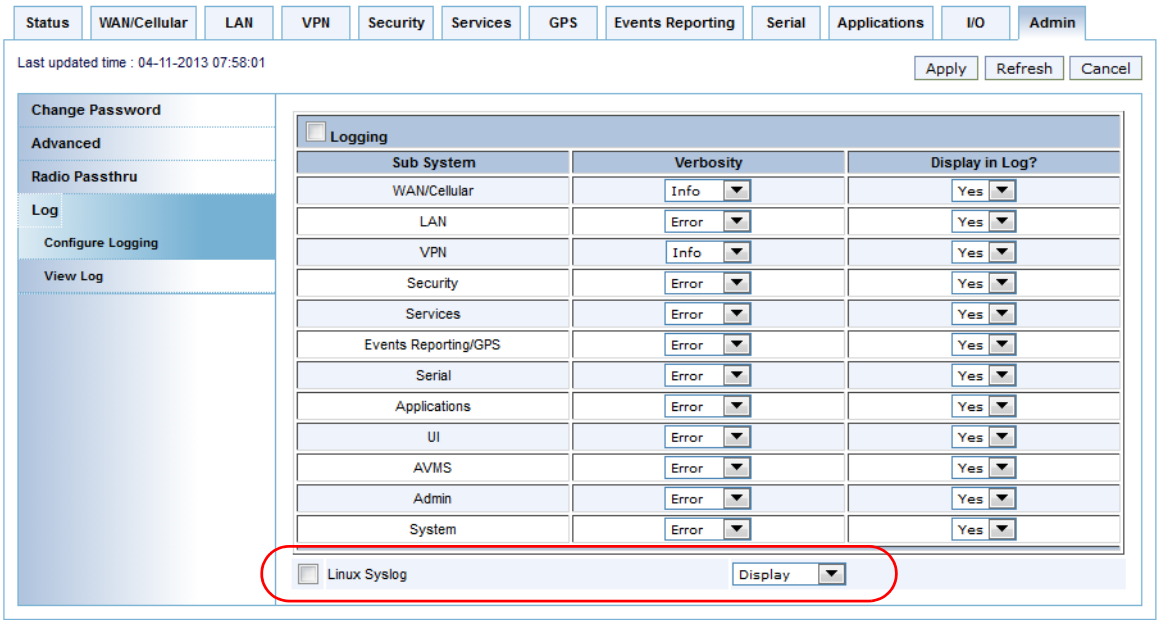
- Ensure that the file name used for the root certificate is home.crt.
- Ensure that you have the correct root certificate for the device you want to communicate with over the VPN.

  Although the same file name is used for all root certificates, each device has its own unique root certificate file. To set up communication with a device over an SSL tunnel VPN, you must load the specific root certificate file for that device.

My VPN connection is not working. When I try to debug it using the logs on the Admin page, VPN information does not show up in the log.

VPN information is collected in the Linux logs. To view this information:

1. Log into ACEmanager as "user" and go to Admin > Log.



2. In the drop-down menu beside Linux Syslog, ensure that Display is selected. If you change the setting:
   a. Click Apply.
   b. Reboot the device.
3. Click View Log.
4. On the View Log page, click Clear and then click Refresh.

Poor Wireless Network Connection

ACE manager indicates that my AirLink device has a poor wireless connection. What can I do to improve it?

For GSM or CDMA networks:

1. Check the RSSI value. If ACEmanager (Status screen) indicates a good RSSI value, go to step 2. If it indicates a poor RSSI value:
   - Check the antenna connection.
   - Make sure you have the correct antenna for the device.
   - You may be in an area with poor coverage. Check with your Mobile Network Operator, or if possible, try moving the AirLink device to a new location.
2. Check the Ec/Io value. If ACEmanager (Status screen) indicates a poor Ec/Io value:
   - This may be a temporary network problem caused by local interference.
   - A nearby laptop or other electronic equipment may be interfering with the signal. Try moving the AirLink device to a different location.

For LTE networks:

1. Check the RSSI value. If ACEmanager (Status screen) indicates a good RSSI value, go to step 2. If it indicates a poor RSSI value:
   - Check the antenna connection.
   - Make sure you have the correct antenna for the device.
   - Try moving the AirLink device to a different location.
2. Check the RSRP value. If ACEmanager (Status screen) indicates a good RSRP value, go to step 3. If it indicates a poor RSRP value:
   - This may be a temporary network problem caused by local interference.
   - Check the antenna connection.
   - Make sure you have the correct antenna for the device.
   - You may be in an area with poor coverage. Check with your Mobile Network Operator, or if possible, try moving the AirLink device to a new location.
3. Check the RSRQ value. If ACEmanager (Status screen) indicates a poor RSRQ value:
   - A nearby laptop or other electronic equipment may be interfering with the signal. Try moving the AirLink device to a different location.

Connection not working

My device appears to be connected to the host, but no data is being transferred.

1. Check to see if MAC filtering is enabled (Security > MAC Filtering).
2. If MAC filtering is enabled:

- Ensure that the MAC Address for the host in question is on the Allowed List.
- Ensure that there are no typos in the MAC Address.

  Or

- If it is not required, disable MAC Filtering and reboot the device.

My host device is unable to connect to the Internet, even when there is good cellular network coverage and ALEOS can Ping an external IP address.

1. Check the DNS proxy setting described on page 94.

   You may need to change this setting to Disable so that all connected hosts acquire the Mobile Network Operator-defined DNS server as the first DNS server. The AirLink device is not used as the DNS resolver.

Updating the ALEOS Software and Radio Module Firmware

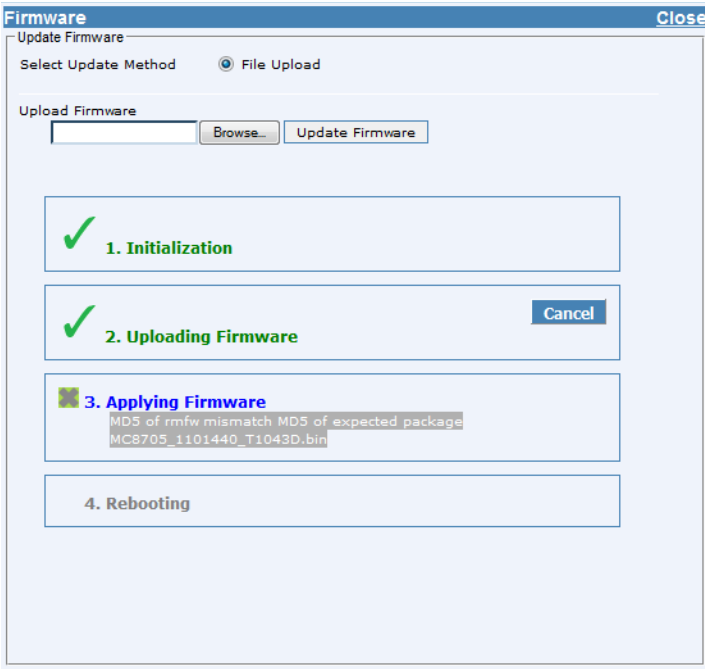
When I am trying to update the radio module firmware, the connection times out and I cannot reconnect to the device.

Depending on the file size and the connection speed, it can take 10 to 20 minutes to upload and install the radio module firmware. While this is taking place, you may see a “connection timed out” message. You can ignore this message, as the

connection is still valid and the firmware update process is continuing. If you are connected to the device over-the-air, you will not be able to access the device until the radio module update is complete.

1. Continue to wait for the process to complete and the device to reboot.
   - **Do Not** reset the device.
   - **Do Not** disconnect the power.
   - **Do Not** click Cancel.
2. If after 20 minutes, the device does not reboot, contact Sierra Wireless Technical Support.

During the radio module firmware update, I see an "X" beside Applying Firmware and a message similar to the following: "MD5 of rmfw mismatch MD5 of expected package MC8705_1101440_T1043D.bin" under Applying Firmware.



The radio module firmware file selected is not the correct one for the device.

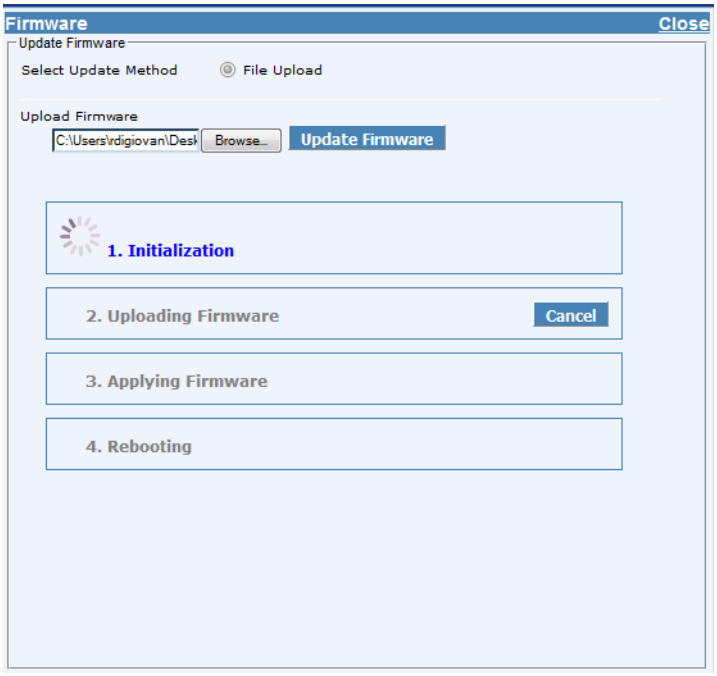
1. Make a note of the file name at the end of the error message. (In this example, MC8705_1101440_T1043D.bin) This is the correct radio module firmware file for the device you are updating.
2. Close the Firmware window.
3. Reboot the device.

   This returns the device to the original ALEOS software and radio module firmware versions.
4. Update the ALEOS software and radio module firmware as described on page 31, using the correct file for the radio module firmware update. (If you do not have the correct file, you can download it from www.sierrawireless.com/Support/Downloads.aspx.)

5. If it still fails, even when you use the correct file, there may have been a problem downloading the file, and it may be corrupted. Download the file again from www.sierrawireless.com/Support/Downloads.aspx and try again.

   If it still fails, contact your FSE or Sierra Wireless Support.

When I try to update the ALEOS software, the process gets "stuck" in the initialization phase.

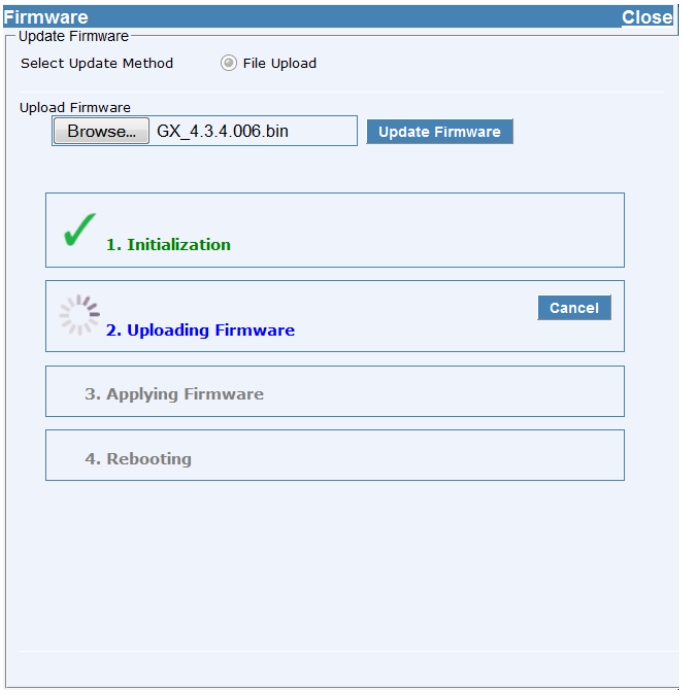


If the update remains in the initialization phase for more than 5 minutes, as shown in the preceding illustration:

1. Close the Firmware window.
2. Reboot the device.

   This returns the device to the original ALEOS software and radio module firmware versions.
3. Update the ALEOS software and radio module firmware as described on page 31.

When I try to update the ALEOS software or the radio module firmware over-the-air, the process appears “stuck” at either the Uploading Firmware or Applying Firmware phase.

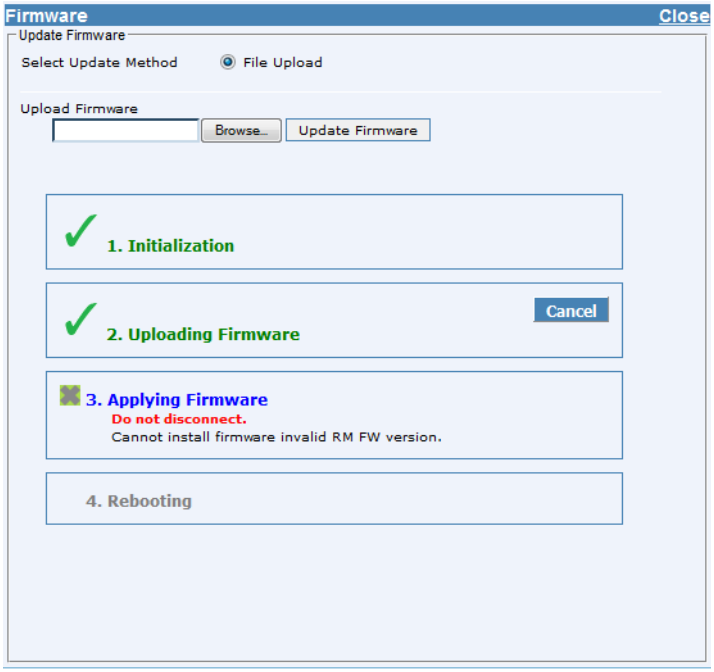


When you are updating the radio module over-the-air, the The radio shuts down during the update and therefore is unable to send the update status to ALEOS.

Wait for the process to complete and the device to reboot. (This could take up to 20 minutes).

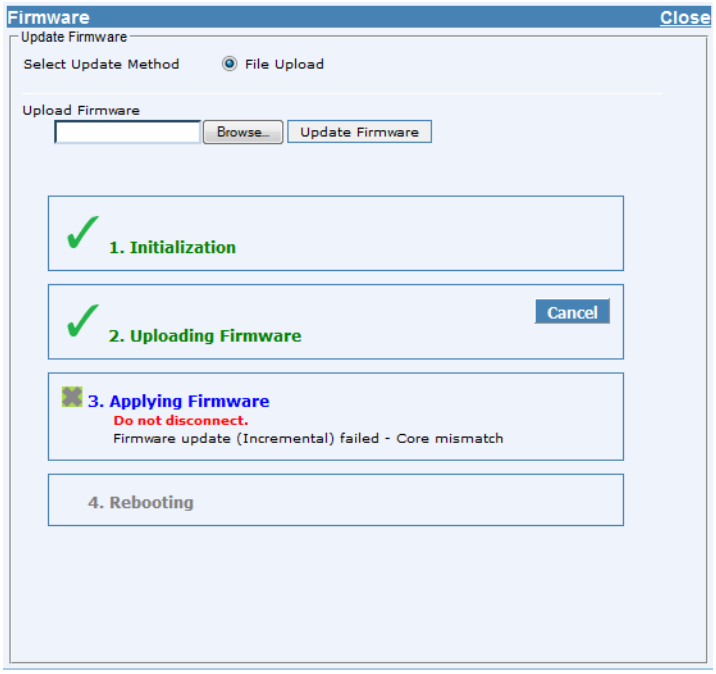
1. Once the device has rebooted, log in to ACEmanager.
2. Go to Status > About and confirm that the software/firmware has been updated.

When I try to update the firmware, I see an “X” beside Applying Firmware and the error message “Cannot install firmware invalid RM FW version”.



The firmware version you are trying to install is not supported by the device. Contact your Sierra Wireless assistance.

When I try to install ALEOS 4.3.2a using ACEmanager, I see the following message: “Firmware update (Incremental) failed - Core mismatch”.



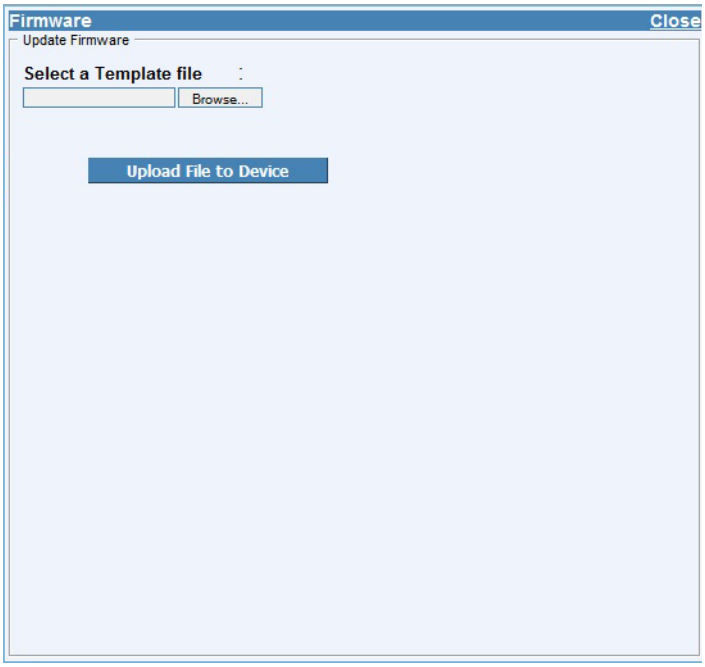
ALEOS 4.3.2 is an important intermediate update step that all devices must go through before you can update them to a version of ALEOS that is newer than 4.3.2.

This message appears when the device you are trying to update has ALEOS version 4.3.1 (or older) and you are attempting to update it to ALEOS 4.3.2a directly without first installing ALEOS 4.3.2.

To correct the problem:

1. Click Cancel.
2. Close ACEmanager, re-launch it, and log in.
3. Click the Firmware link
4. First update to ALEOS 4.3.2, and then update to ALEOS 4.3.2a-I. (For detailed instructions, see page 28.)

When I open the Firmware window, part of it appears to be missing.



If the Firmware window is not displaying properly:

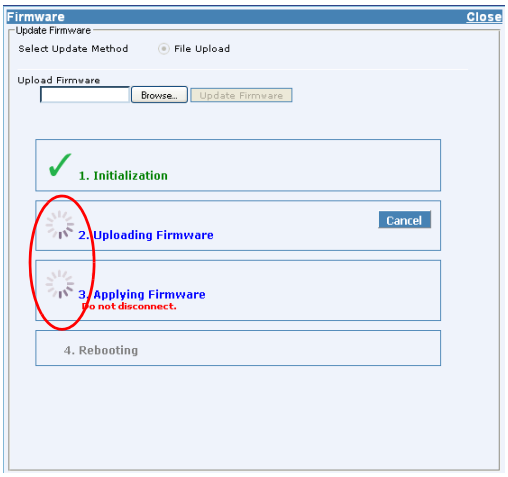
- Reboot the device and try again.

  Or

- Close ACEmanager, reopen it in Firefox® (rather than Internet Explorer®) and try again.

When I run the firmware update, it looks as if the device is applying the firmware before the firmware upload is complete. Is this going to prevent the firmware from updating properly?

This is a known issue in the User Interface. The firmware update is not affected. Even though the progress circle beside Uploading Firmware does not change to a check mark before the next process circle appears beside Applying Firmware, the firmware upload does complete before the device begins applying the firmware.



When I try to update the radio module using AVMS, I receive an error message.

The following table provides a brief explanation of the firmware update error messages.

Error message	Meaning	Corrective action
Cannot Install Firmware	The system has encountered errors from which it cannot recover and requires at least a reboot before trying to update again.	Press the reset button for 20 seconds to reset the device to the factory default settings and try again. If it still does not work, contact AVMS support[a].
Link not up in 3 minutes...Exiting	The radio module was not able to establish the connection in 3 minutes. The update has been aborted, but can be relaunched as soon as the connection is OK.	Wait for network connectivity and then try again.
Unable to download JUD file from <url>	The URL is wrong, or the download failed (interruption, no space left...).	Contact AVMS support[a].
Core version not found in JUD file	JUD file is not valid. Core Version is a mandatory field.	There is a problem with the package on the AVMS server. Contact AVMS support[a].
Required information (URL, Size or MD5) is missing from JUD file	JUD file is not valid. URL, Size, and MD5 sum of the firmware package are mandatory fields.	There is a problem with the package on the AVMS server. Contact AVMS support[a].
Cannot perform upgrade — No space left on device	Firmware is larger than available space for the download.	Contact AVMS support[a]. The support team will need to access the device to clear space, or you can return the device to Sierra Wireless under an RMA.
Unable to download ALEOS firmware from <url>	Firmware URL is not valid, or the download failed.	Retry. If the download fails several times, contact AVMS support[a]. The support team will need a log from the device.
Undefined ALEOS firmware URL	ALEOS firmware URL not specified, so firmware cannot be retrieved.	Contact AVMS support[a] to confirm that there is not a problem with the service.

Error message	Meaning	Corrective action
ALEOS firmware MD5 check failed	The downloaded firmware package failed the integrity check. The update is aborted.	There is a problem with the package on the device or the download may have failed. Restart the firmware download. If the problem persists, contact AVMS support[a]. There may be a problem with the package on the AVMS server.
Unable to apply ALEOS firmware and Unable to apply ALEOS firmware (retry)	ALEOS firmware could not be applied. Check the ALEOS log messages to determine exactly why the update failed.	Retry. If the problem persists, contact AVMS support[a] and provide them with the log messages.
Radio Module URL is missing from JUD file	JUD file is not valid. The Radio Module Firmware URL is a mandatory field.	There is a problem with the package on the AVMS server. Contact AVMS support[a].
Radio Module package MD5 sum is missing from JUD file	JUD file is not valid. The Radio Module Firmware MD5 sum is a mandatory field.	There is a problem with the package on the AVMS server. Contact AVMS support[a].
Radio Module firmware MD5 check failed	The downloaded firmware package failed the integrity check. The update is aborted.	There is a problem with the package on the device or the download may have failed. Try downloading the file again. If the problem persists, contact AVMS support[a]. There may be a problem with the package on the AVMS server.
Radio Module backup failed	The radio module was saved to prevent a power failure. If the firmware cannot be backed-up on persistent storage, the firmware update will not proceed because of the risk that the radio module update will not be able to finish if interrupted.	Contact AVMS support[a]. The support team will need to access the device to clear space, or you can return the device to Sierra Wireless under an RMA.
Radio Module firmware download failed	Firmware URL is not valid, or download failed.	Retry several times. If the problem persists, contact AVMS support[a]. The support team will need a log from the device.
Undefined Radio Module firmware URL	The URL cannot be retrieved. The update is aborted.	Retry. If the problem persists, contact AVMS support[a].
Radio Module firmware update failed	Radio module firmware could not be applied. Check the ALEOS log messages to determine exactly why the update failed.	Retry. If the problem persists, contact AVMS support[a].

a. AVMS technical support: https://issues.m2mop.net

TCP Connections

I went to the TCP section of the Serial screen and configured ALEOS to include the Device ID in TCP connections, but I get the message “Device ID Not Set”.

Setting the TCP connection to include the Device ID is a two step process:

1. In ACEmanager, go to Serial > TCP and ensure that the Include Device ID on TCP Connect field is set to Enable.

   (See Port Configuration on page 221.)

2. Go to GPS > Global Settings > General and configure the Use Device ID in Location Reports field. (See Global Settings on page 204.)

To confirm that the Device ID is configured, check the Status > About screen. The Device ID, if set, appears in the GPS/RAP Device ID field.

AirVantage Management Service

I don't understand the message that appears in the Status field in the Services > AVMS window.

The error messages in the Services > AVMS > Status field can be due to a communication failure, a problem with the AVMS server, or a failure when parsing a valid AVMS server response. The following table describes the error messages and the corrective action.

Error message	Meaning	Corrective action
Communication Failure Errors		
Initialization error	The transfer object could not be initialized.	Contact AVMS support[a].
Unsupported protocol	The AVMS server URL protocol is not supported.	In ACEmanager, check the AVMS URL in the Service > AVMS > Server URL field. The default value is http://na.m2mop.net/device/msci/com.
Failed initialization	The transfer library could not be initialized.	Contact AVMS support[a].
URL using bad/illegal format or missing URL	The AVMS server URL is missing or not properly formatted.	In ACEmanager, check the AVMS URL in the Service > AVMS > Server URL field. The default value is http://na.m2mop.net/device/msci/com.
Couldn't resolve host name	The AVMS server URL could not be resolved.	In ACEmanager, check the AVMS URL in the Service > AVMS > Server URL field. The default value is http://na.m2mop.net/device/msci/com. Also check the cellular connectivity.
Couldn't connect to server	Connection to the AVMS server URL failed.	In ACEmanager, check the AVMS URL in the Service > AVMS > Server URL field. The default value is http://na.m2mop.net/device/msci/com. Also check the cellular connectivity.
Timeout was reached	The transfer timeout (equal to the communication period if defined or 5 minutes) expired.	Check cellular connectivity.
Server returned nothing (no headers, no data)	No data was received from the AVMS server.	Check cellular connectivity.
Unrecognized or bad HTTP Content or Transfer-Encoding	The AVMS server http response contains a mal-formed content or transfer-encoding header field.	Contact AVMS support[a].
Out of memory	A memory allocation problem occurred.	Contact AVMS support[a].
AVMS Server Errors		

Error message	Meaning	Corrective action
HTTP error '500'	AVMS server reported error 500 in the HTTP response.	Refer to the available AVMS server documentation for a list of all possible error codes and their significance.
Error message indicating a failure when parsing a valid AVMS server response		
XML processing error	The content of a valid AVMS server response cannot be parsed.	AVMS server responses are mal-formatted. Contact AVMS support[a].

a. AVMS technical support: https://issues.m2mop.net

LTE Networks

How do I interpret the number shown in the Band Class field on the Status > WAN Cellular window for a device on an LTE network?

Use the following table to interpret the values in the LTE Band Class field in ACEmanager (STATUS > WAN Cellular).

Band Class number	Uplink frequency range (MHz)	Downlink frequency range (MHz)
120	1920–1980	2110–2170
121	1850–1910	1930–1990
122	1710–1785	1805–1880
123	1710–1755	2110–2155
124	824–849	869–894
125	830–840	875–885
126	2500–2570	2620–2690
127	880–915	925–960
128	1749.9–1784.9	1844.9–1879.9
129	1710–1770	2110–2170
130	1427.9–1452.9	1475.9–1500.9
131	698–716	728–746
132	777–787	746–756
133	788–798	758–768
134–135	Reserved for bands 15 and 16	
136	704–716	734–746
137	815–830	860–875
138	830–845	875–890

Band Class number	Uplink frequency range (MHz)	Downlink frequency range (MHz)
139	832–862	791–821
140	1447.9–1462.9	1495.9–1510.9
141–151	Reserved for bands 22 to 32	
152	1900–1920	1900–1920
153	2010–2025	2010–2025
154	1850–1910	1850–1910
155	1930–1990	1930–1990
156	1910–1930	1910–1930
157	2570–2620	2570–2620
158	1880–1920	1880–1920
159	2300–2400	2300–2400

How do I obtain and interpret SINR values for LTE networks?

You can use the AT*CELLINFO? command to obtain an SINR (Signal to Interference plus Noise Ratio) value. (See *CELLINFO2? on page 323.)

The values vary depending on the network characteristics and the AirLink device, but in general, a positive value provides usable throughput. The following table provides guidelines for interpreting SINR values.

SINR Value	Throughput
< 0	Poor
0 to 5	Fair
6 to 10	Good
> 10	Excellent

If the SINR value indicates poor throughput:

- Move the antenna away from noisy equipment.
- Move closer to the nearest cell tower line of sight, or further away from the interfering cell tower.

SIM Card is Blocked

My SIM card has a PIN number. I've entered the wrong PIN several times and now the SIM card is blocked.

AirLink products do not support Personal Unlocking Key (PUK) entry. However, if you need to unblock the SIM card:

1. Contact your Mobile Network Operator to obtain the PUK.

2. Remove the SIM card from the AirLink device and insert it in a cell phone that accommodates a MiniSIM (2FF) card.
3. Enter the PUK to unblock the SIM card and then return the SIM card to the AirLink device.

Note: Be careful when entering the PUK. You have a limited number of attempts to enter the correct PUK (generally 10) before the SIM card is permanently disabled and a new SIM card is required. If the PUK does not unblock the SIM card after the first few attempts, contact your Mobile Network Operator.

Remote connections

I cannot connect to the AirLink device remotely over the Mobile Network Operator's Private Network via the Web UI, although I can connect to it locally.

Some Mobile Network Operators' private networks have restrictions on the maximum transmission unit (MTU) size. This is more prevalent with LTE networks.

Possible solutions:

- Use your Mobile Network Operator's public network.
- Ask your Mobile Network Operator to reduce the MTU size on the router or other equipment at their end of the private network. Setting the MTU value below 1500 bytes (for example 1326 bytes) has resolved the problem on some private networks.
- If your AirLink device has a radio module (such as the MC7700 or MC7750) that supports LTE networks, select an option in ACEmanager (WAN/Cellular > Advanced > Setting for Band field) that excludes LTE networks.

Radio Band Selection

I set the radio band in the UI (WAN/Cellular > Setting the Band) or by using the AT!BAND AT command, but after I reboot the band setting reverts to its former value.

For some SIM cards, you need to set the band before inserting the SIM card.

To resolve this problem:

1. Remove the SIM card.
2. Set the band to the desired value.
3. Reboot the device.
4. Insert the SIM card.

Reliable Static Routing (RSR)

I launched ACEmanager with Internet Explorer 9. I configured RSR, but after I enabled RSR and clicked Apply, all the values reverted to the defaults.

There is a known issue. If you configure and enable RSR with ACEmanager in Internet Explorer 9, and then click Apply, the values in the ACEmanager screen appear as default values.

This is an ACEmanager display issue only. The configuration is applied properly, but the configured values are not displayed. Click Refresh to view the configured values.

G: Glossary of Terms

G

Acronym or Term	Definition
1xEV-DO	Single Carrier (1X) EVolution–Data Only A high-speed standard for cellular packet data communications. It supports Internet connections with data rates up to 3.1 Mbps. (downlink from the network) and 1.8 Mbps (uplink to the network). Average data rates are approximately: • Rev. A: 600-1300 kbps. (downlink from the network) and 300-400 kbps (uplink to the network) • Rev. 0: 400-700 kbps (downlink from the network) and 40-80 kbps (uplink to the network) Actual speed depends on the network conditions. Compare to 1X.
1X	Single Carrier (1X) Radio Transmission Technology A high-speed standard for cellular packet data communications. 1x supports Internet connections with data rates up to 153 kbps (simultaneously in each direction—downlink and uplink). Actual speed depends on the network conditions. Compare to 1xEV-DO.
3GPP	3rd Generation Partnership Project 3GPP unites 6 telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TTA, TTC), and provides their members with a stable environment to produce Reports and Specifications that define 3GPP technologies.
API	Application Programming Interface A protocol intended to be used as an interface by software components to communicate with each other.
AT	A set of device commands, preceded by “AT” originally developed by Hayes, Inc. for their devices. The structure (but not the specific commands, which vary greatly from manufacturer to manufacturer) is a de facto device industry standard.
CDG	CDMA Development Group A consortium of companies who joined together to lead the adoption and evolution of CDMA wireless systems around the world. Also see CDMA.
CDMA	Code Division Multiple Access A wideband spread spectrum technique used in digital cellular, personal communications services, and other wireless networks. Wide channels (1.25 MHz) are obtained through spread spectrum transmissions, thus allowing many active users to share the same channel. Each user is assigned a unique digital code, which differentiates the individual conversations on the same channel.
cdmaOne	A IS-95 CDMA standard developed by QUALCOMM Inc. Also known as TIA-EIA-95.

Acronym or Term	Definition
CE, CE Label	The CE label is a mandatory conformity marking for products placed on the market in the European Economic Area (EEA). With the CE marking on a product, the manufacturer declares that the product conforms with the essential requirements of the applicable EC directives.
CnS	Sierra Wireless' proprietary Control and Status protocol interface
DCE	Data Communications Equipment A device that sits between the data terminal equipment (DTE) and a data transmission circuit. Usually the DCE is a modem.
Diversity	Antenna diversity, also called space diversity, is a scheme that uses two or more antennas to improve the quality and reliability of a wireless link. Often, especially in urban and indoor environments, there is no clear line-of-sight (LOS) between transmitter and receiver. Instead the signal is reflected along multiple paths before finally being received. Each bounce can introduce phase shifts, time delays, attenuations, and distortions that can destructively interfere with one another at the aperture of the receiving antenna.
EDGE	Enhanced Data rates for GSM Evolution A digital mobile phone technology that allows improved data transmission rates as a backward-compatible extension of GSM. EDGE is considered a pre-3G radio technology and is part of ITU's 3G definition. Also known as Enhanced GPRS (EGPRS), or IMT Single Carrier (IMT-SC), or Enhanced Data rates for Global Evolution.
EIA	Electronics Industry Association EIA was a standards and trade organization composed as an alliance of trade associations for electronics manufacturers in the United States. They developed standards to ensure the equipment of different manufacturers was compatible and interchangeable. The EIA ceased operations on February 11, 2011, but the former sectors continue to serve the constituencies of EIA.
EMC	Electromagnetic Compatibility The branch of electrical science which studies the unintentional generation, propagation and reception of electromagnetic energy with reference to the unwanted effects (Electromagnetic interference, or EMI) that such energy may induce.
EMI	Electromagnetic Interference The disturbance that affects an electrical circuit due to either electromagnetic induction or electromagnetic radiation emitted from an external source
ERP	Effective Radiated Power A standardized theoretical measurement of radio frequency (RF) energy. It is determined by subtracting system losses and adding system gains.
ESN	Electronic Serial Number The unique first-generation serial number assigned to AirLink devices for use on the wireless network. Compare to MEID.
Ethernet	Computer networking technologies for local area networks (LANs).
EU	The European Union Organization of European countries.

Acronym or Term	Definition
EVDO	Enhanced Voice-Data Optimized or Enhanced Voice-Data Only (Ev-DO, EV, EVDO, etc.). A telecommunications standard for the wireless transmission of data through radio signals, typically for broadband Internet access. It uses multiplexing techniques including code division multiple access (CDMA) as well as time division multiplexing (TDM) to maximize both individual users' throughput and the overall system throughput.
FCC	Federal Communications Commission The U.S. federal agency responsible for interstate and foreign communications. The FCC regulates commercial and private radio spectrum management, sets rates for communications services, determines standards for equipment, and controls broadcast licensing.
FW	Firmware Software stored in ROM or EEPROM; essential programs that remains even when the system is turned off. Firmware is easier to change than hardware but more permanent than software stored on disk.
GPRS	General Packet Radio Service A packet-oriented mobile data service on 2G and 3G cellular communication systems. GPRS was originally standardized by European Telecommunications Standards Institute (ETSI) in response to the earlier CDPD and i-mode packet-switched cellular technologies. It is now maintained by the 3rd Generation Partnership Project (3GPP).
GPS	Global Positioning System A system that uses a series of 24 satellites to provide navigational data.
GSM	Global System for Mobile Communications (originally Groupe Spécial Mobile) GSM is a standard developed by the European Telecommunications Standards Institute (ETSI) to describe protocols for second generation (2G) digital cellular networks used by mobile phones
HSPA	High Speed Packet Access An amalgamation of two mobile telephony protocols: High Speed Downlink Packet Access (HSDPA) and High Speed Uplink Packet Access (HSUPA). This extends and improves the performance of existing 3rd generation mobile telecommunication networks utilizing the WCDMA protocols.
HSPA+	Also called evolved HSPA This allows bit-rates to reach as high as 168 Mbit/s in the downlink and 22 Mbit/s in the uplink. An improved 3GPP standard.
IC	Industry Canada The government department responsible for overseeing and regulating wireless and communication technologies in Canada.
IEC	International Electrotechnical Commission A non-governmental international standards organization that prepares and publishes International Standards for all electrical, electronic and related technologies – collectively known as "electrotechnology.”

Acronym or Term	Definition
IOTA	Internet Over The Air An automated feature, supported by some service providers, to perform account setup by making a connection to the CDMA network and using a secure Internet connection to download account parameters to the device.
IS	Interim Standard After receiving industry consensus, the TIA/EIA forwards the standard to ANSI for approval.
IS-95	A 2G mobile telecommunications standard using CDMA to send voice, data and signaling data (such as a dialed telephone number) between mobile telephones and cell sites.
ITU	International Telecommunication Union A specialized agency of the United Nations responsible for issues that concern information and communication technologies. The ITU coordinates the shared global use of the radio spectrum, promotes international cooperation in assigning satellite orbits, and assists in the development and coordination of worldwide technical standards.
kbps	Kilobits per second 1000, not 1024, as used in computer memory size measurements of kilobytes.
LED	Light Emitting Diode A semiconductor diode that emits visible or infrared light.
LTE	Long Term Evolution High performance air interface for cellular mobile communication systems.
Mbps	Millions of bits per second, or Megabits per second.
MEID	Mobile Equipment IDentifier The unique second-generation serial number assigned to the device for use on the wireless network. *Compare to* ESN.
NAM	Number Assignment Module Semi-permanent information stored in the device's non-volatile memory, including the device's Mobile Identification Number, the station class mark, Mobile Network Operator code, and other cellular identifiers. Essentially the phone number, it should be treated as confidential information and should not be disclosed to anyone other than the cellular service provider.
NV	Non-Volatile (memory)
OEM	Original Equipment Manufacturer A company that manufactures a product and sells it to a reseller.
OTAPA	Over the Air Parameter Administration A way of distributing new software updates or configuration settings to devices like cellphones and set-top boxes.
OTASP	Over the Air Service Provisioning. Also see OTAPA.
PCS	Personal Communications Services A cellular communication infrastructure that uses a different frequency range than AMPS.

Acronym or Term	Definition
PPP	Point to Point Protocol An alternative communications protocol used between computers, or between computers and routers on the Internet. PPP is an enhanced SLIP. Also see SLIP.
PRI	Product Release Instructions A file containing the settings used to configure devices for a particular service provider, customer, or purpose.
RF	Radio Frequency
RoHS	Restriction of use of Hazardous Substances mandated by EU Directive 2002/95.
RS-232	A series of standards for serial binary single-ended data and control signals connecting between a DTE (Data Terminal Equipment) and a DCE (Data Circuit-terminating Equipment). It is commonly used in computer serial ports.
Rx	Receive
SIM, SIM Card	Subscriber identity module or subscriber identification module. An integrated circuit which securely stores the international mobile subscriber identity (IMSI) and the related key used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers).
SINR	Signal to Interference plus Noise Ratio (SINR) is an RF parameter that is directly proportional to throughput (the higher the number, the higher the throughput). It can help LTE radio installers gauge the signal quality between the cell tower and the radio module. For more information on interpreting the SINR values, see How do I obtain and interpret SINR values for LTE networks? on page 397.
SKU	Stock Keeping Unit Identifies an inventory item: a unique code, consisting of numbers or letters and numbers, assigned to a product by a retailer for purposes of identification and inventory control.
SLIP	Serial Line Internet (or Interface) Protocol An Internet Protocol designed to work over serial ports and modem connections. On personal computers, SLIP has been largely replaced by the Point-to-Point Protocol (PPP), which has more features and does not require its IP address configuration to be set before it is established. On microcontrollers SLIP is still the preferred way of encapsulating IP packets due to its very small overhead. Also see PPP.
SMS	Short Message Service A feature which allows users of a wireless device on a wireless network to receive or transmit short electronic alphanumeric messages (up to 160 characters, depending on the service provider).
TIA / EIA	Telecommunications Industry Association / Electronics Industry Association A standards setting trade organization, whose members provide communications and information technology products, systems, distribution services and professional services in the United States and around the world.
Tx	Transmit

Acronym or Term	Definition
UMTS	Universal Mobile Telecommunications System (UMTS). A third generation mobile cellular system for networks based on the GSM standard. Developed and maintained by the 3GPP (3rd Generation Partnership Project), UMTS is a component of the International Telecommunications Union IMT-2000 standard set and compares with the CDMA2000 standard set for networks based on the competing cdmaOne technology.
USB	Universal Serial Bus An industry standard defining the cables, connectors and communications protocols used in a bus for connection, communication and power supply between computers and electronic devices.

Index

A

access points
  maximum number configurable for GX 90
  mode 86
ACEmanager 146
  configuring 18
  description 13
  login 17
  overview 13
ACEview 286
ALEOS Application Framework
  troubleshooting 383
  unable to load application from 383
  using 250
ALEOS software update 28
analog inputs
  channel
    configuration 324
  transformed values 258
  uses 253
APN 107
  backup 119
applications 243
AT Commands
  Applications > Data Usage 372
  GPS > Server 1 - Server 4 353
  I/O > Current State 371
  LAN/WiFi > DHCP/Addressing 334
  Security > Trusted IPs - Inbound 339, 344
  Serial > Port Configuration 360
  Services > Low Power 345
  Status > Home 323, 366
  summary 321
  using 321
  Wi-Fi 336
AVMS
  configuration 145
  error messages 393

C

client mode 90
configuration
  application 243
  events reporting 207
  GPS 185
  LAN 67
  logging 264
  serial 221
  services 145
  VPN 123
  WAN/Cellular 103
  Wi-Fi 67
Connection not working 386

D

data usage 243
Dead Peer Detection 127
Device Status Screen 183
DHCP/Addressing 70
Dial-up Networking 267
digital inputs
  GX Series 254
  LS300 254
  uses 253
DMZ 137
DNS
  dynamic 151
  global 93
DNS proxy
  configure 94
  status 48, 50, 52, 54
documentation 14, 15
domain name 155
dual mode Wi-Fi 92
DUN
  operating systems supported 267
  setting up 267

E

EC/IO 45
email
  SMTP 176
  test 174
engine hours 212
error reporting, troubleshooting 384
ethernet
  and DMZ 138
  and host connection mode 72
  AT commands 324
  MAC address 65
  status 55, 57
  troubleshooting 381
  troubleshooting LEDs 381
  virtual port 80
ethernet ports 74
  troubleshooting 381
events reporting configuration 207

F

firmware update 28

G

Garmin 248
global DNS 93
Glossary 401
GPS
  configuration 185

global settings 204
streaming 383
troubleshooting 383
GRE 128
H
Host Interface Watchdog 101
host port routing 38, 84
I
Internal DHCP Server 73
IP Manager 154
IPsec 123, 125
K
keepalive 116
L
LAN configuration 67
LAN management 37
LEDs, above Ethernet port 381
Load Root Certificate 132
Local/Streaming 198, 201
logging configuration 264
login 17
low power mode 147
LTE Band Class field 396
M
MAC filtering 142, 386
MIB (Management Information Base) 295
Modbus 234, 289
Modbus address list 234
Modbus TCP/IP 290
N
network connection, poor 385
Network State 43
NMEA 186
O
Over the Air (OTA) connections 38
P
packet inspection 143
PAD mode 22
password, change 261
PCI compliance 38
ping, on demand 263
port filtering
inbound 139
outbound 140
port forwarding 133
error message 382
troubleshooting 382
PPP connection, configuring 234
PPPoE 94
Programmable Logic Controller 290
public and private mode 67
pulse count 256
R
radio band, selecting 109, 398
radio module firmware update 28
radio passthru 263
RAP 186
re-activation 118
redundant server 196
relay outputs 254
Reliable Static Routing (RSR) 119
Remote Terminal Unit 289
reset
periodic and time of day 263
reverse telnet/SSH 224
RSRP 44
RSRQ 45
RSSI 44
S
security configuration 133
serial configuration 221
serial port
port configuration 223
PPP 234
TCP 230
UDP 232
virtual 81
services configuration 145
Simple Network Management Protocol (SNMP) 177
SINR 397
SMS 157
advanced 173
Control and Gateway mode 164
Control Only mode 159
Gateway Only mode 161
M2M 174
Password 171
Password Only mode 158
password, default 172
Quick Test 174
security 169
test 174
troubleshooting 383
trusted phone number 171
SMS Commands 377
SMS M2M 174
SMS message error 383
SMS Wakeup 168
SNMP traps 295
SNTP 182
split tunnel 124
SSH 175
SSL tunnel 129
Status
About 64

Applications 64
GPS 60
Home 41
LAN 55
LAN/WiFi 56
Security 59
Serial 62
Services 59
VPN 58
WAN/Cellular 47

T

TAIP 186
TCP connection
configuring 230
Device ID Not Set 394
settings 239
troubleshooting 393
telemetry 289
Telnet 175
template
applying 20
creating 19
test button, SMS/email 174
third party services 153
time (SNTP) 182
troubleshooting
ALEOS AF 383
ALEOS software update 386, 388, 389, 391, 392
AVMS error messages 393
AVMS status messages 395
Dual Ethernet X-Card 381
error reporting 384
ethernet ports 381
GPS 383
port forwarding 382
radio module firmware update 386, 387, 390, 392
SMS 383
TCP connections 394
VPN 384
Wi-Fi X-Card 382
wireless connection 385, 386
trusted IPs
inbound 140
outbound 142
Trusted Phone Number 171

U

UDP connection
configuring 232
settings 241
UDP Multiple Unicast 227
update
ALEOS software 28
radio module firmware 28
USB drivers, installing 78
USB port 76

V

VLAN 99
VPN
configuration 123
troubleshooting 384
VPN 1 tunnel 124
VRRP 100

W

WAN/Cellular configuration 103
WEP encryption, troubleshooting 382
Wi-Fi
Access Point Mode 86
Both (AP + Client) Mode 92
Client Mode 90
dual mode 92
modes 85
troubleshooting 382
Wi-Fi configuration 67
WiFi Landing Page 157

X

X-Card
applying template 20
configuration 235
Dual Ethernet 55, 65, 72, 76, 138
Dual Ethernet, AT command 324
Dual Ethernet, troubleshooting 381
I/O 211, 217, 254, 255
I/O serial port configuration 235
I/O, AT command 371
I/O, relay output and 256
Serial port 63
status 46
type 46
Wi-Fi 67, 72, 101, 157
Wi-Fi, AT command 338
Wi-Fi, troubleshooting 382

SIERRA
WIRELESS™